

Chapter 5

Examples of groups

Introduction

In this book we discuss groups. Much of the early material should be familiar from your previous studies. The main aim of the book is to introduce results that can be used to describe the structure of finite groups.

In mathematics, a description of an infinite class of mathematical objects often comes in the form of a *classification*, that is, a list where the objects in question are grouped into finitely many categories according to some structural characteristics. Thus, the most general problem that we could pose for finite groups asks for a classification of them. Unfortunately, this problem seems hopelessly hard, but less general classification results can be obtained by imposing some additional conditions on the finite groups under consideration.

It is the importance of finite groups in applications, as well as in other branches of mathematics, that motivated the interest in a classification: finite groups provide sophisticated tools for the study and analysis of patterns of all sorts, for example the patterns found in the solutions to polynomial equations, the patterns found in the symmetries of crystals, and more recently certain patterns found in viruses.

A finite group G is said to be *simple* if its only normal subgroups are the identity subgroup and G itself. This means, in some sense, that a group is simple if it cannot be decomposed into two smaller groups. Simple groups are very important in classification: there is a theorem, proved by Jordan (1838–1922) and Hölder (1859–1937) towards the end of the nineteenth century, that tells us that finite simple groups are the building blocks of finite groups, rather like prime numbers are the building blocks of the integers. This is why much of the work on finite groups in the latter half of the twentieth century was about trying to identify all finite *simple* groups.

The classification of finite simple groups was finally achieved around 2004, after a joint effort that stretched over 50 years and involved many mathematicians, but the details are well beyond the scope of this module. However, by the end of the book you should be familiar with several classes of groups and be able to determine the possible structures for groups of some given orders.

This chapter introduces some basic features of groups. In Section 1 you are reminded of the group axioms, and of groups arising from symmetries of plane figures and from modular arithmetic. You will review subgroups and cosets in Section 2, and normal subgroups and quotient groups in Section 3. Section 4 covers group isomorphisms and homomorphisms. Lagrange's Theorem, the First Isomorphism Theorem and the Correspondence Theorem are stated and proved in Sections 2 and 4. In the final section you will work in some detail with the group of permutations on four elements. The exercises in this section provide a concrete illustration of the ideas of the whole chapter.

Chapter guide

In this chapter, we assume you have some familiarity with groups and their basic properties from your previous studies. One of the aims is to introduce you to many examples of both finite and infinite groups that will recur later in Book B. Some of these examples help to highlight the fact that groups can have several different but equivalent representations. This is the longest chapter in Book B, but a lot of the material will be revision.

The first three sections are of roughly equal length and should mostly be revision. The last part of Section 4 proves the Correspondence Theorem, an important result you should make sure you are familiar with. Section 5 consists mostly of exercises designed to apply the notions of the first four sections to a specific finite group.

1 Axioms and examples

This section reminds you of the axioms for a group and looks at some examples that will prepare you for the rest of the chapter. Some of the examples may be familiar to you, some may not be. Since this topic demands real familiarity with many of these examples, we ask you to work carefully through all the exercises.

1.1 Group axioms

You may remember from your previous studies that the group axioms are an abstraction of certain properties shared by various sets of numbers, functions, transformations, etc., equipped with an operation to combine the elements of the set. The abstraction process leads to the following definition.

Definition 1.1 *Group axioms*

A set G together with a binary operation $\circ$ defined on G is a **group** if the following axioms are satisfied.

G1 Closure For all pairs x, y of elements in G , $x \circ y$ is also in G .

G2 Identity There is an **identity element** e , say e in G with the property that, for any element x in G ,

$$e \circ x = x = x \circ e.$$

G3 Inverses For each element x in G , there is an **inverse element** x^{-1} in G with the property that

$$x \circ x^{-1} = e = x^{-1} \circ x,$$

where e is the identity element of G .

G4 Associativity For all choices of elements x, y, z in G , we have

$$(x \circ y) \circ z = x \circ (y \circ z).$$

Although the closure axiom follows from the definition of a binary operation, we include it for clarity.

The set G is sometimes called the **underlying set** of the group, and we should really say that $(G, \circ)$, rather than G , is a group if the axioms are satisfied; that is, we should always make explicit reference to the set *and* the operation when talking about groups. However, to avoid clumsiness, we will follow convention and refer to ‘the group G ’ whenever the operation that makes the set into a group is clear from the context. We usually write the group operation as if it were multiplication: we write xy where we should, strictly, write $x \circ y$. The main exception to this rule will be where the group operation is called addition, in which case we write $x + y$.

There are several elementary consequences of these axioms that you will have seen when you were first introduced to groups. You may have noticed, for example, that the phrase ‘an identity’ in the second axiom has become ‘the identity’ in the third. This follows from the fact that a group can have only one identity. For ease of reference, the elementary consequences that you are expected to know are summarised in the following proposition.

Proposition 1.2 *Elementary consequences of the group axioms*

Let G be a group.

(a) **Uniqueness of identity**

The identity element of G is unique.

(b) **Uniqueness of inverses**

Let a be an element of G . Then the inverse of a is unique.

(c) **Left cancellation rule**

For any elements x, y and a of G ,

$$ax = ay \quad \text{implies} \quad x = y.$$

(d) **Right cancellation rule**

For any elements x, y and a of G ,

$$xa = ya \quad \text{implies} \quad x = y.$$

(e) **Inverse of a product**

For any elements x and y of G , the inverse of the product xy is $y^{-1}x^{-1}$.

Proposition 1.2(e) says that

$$(xy)^{-1} = y^{-1}x^{-1}.$$

The fact that there is a reversal of order in the inverse of a product may seem strange initially. However, consider the process of putting on your shoes and socks. The reverse process (*inverse*) clearly involves taking off your shoes before taking off your socks!

Worked Exercise 1.3

Show that the set of the integers with addition, $(\mathbb{Z}, +)$, is a group.

Solution

We check the axioms.

Closure The sum of two integers, positive or negative, is another integer.

Identity The integer 0 is the identity element for addition: for any integer x ,

$$x + 0 = x = 0 + x.$$

Inverses The inverse of an integer x is the integer $-x$, because $x + (-x) = 0 = (-x) + x$ and 0 is the identity element of $\mathbb{Z}$.

Associativity From what we know about addition, it is the case that $(x + y) + z = x + (y + z)$ for all choices of integers x , y and z .

You will know from your previous studies that the sets of numbers $(\mathbb{Q}, +)$, $(\mathbb{Q} \setminus \{0\}, \times)$, $(\mathbb{R}, +)$, $(\mathbb{R} \setminus \{0\}, \times)$, $(\mathbb{C}, +)$, $(\mathbb{C} \setminus \{0\}, \times)$ are groups. We will not show the details here.

Exercise 1.1

Check that each of the following sets, with the given operation, forms a group. For each example, you should specify the identity of the group and how to find an inverse for each element. You may assume that matrix multiplication is associative.

- (a) Set: all 2×2 matrices with real numbers as entries and non-zero determinant.

Operation: matrix multiplication.

- (b) Set: all 2×2 matrices of the form

$$\begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}, \quad a \in \mathbb{Z}.$$

Operation: matrix multiplication.

The group in Exercise 1.1(a) is an important example called the **general linear group** $\text{GL}(2, \mathbb{R})$. The word ‘linear’ is used because matrices represent linear transformations between vector spaces. The 2 indicates the size of the matrices, and the $\mathbb{R}$ indicates that the entries are real numbers.

Exercise 1.2

Let G be a group, and let x and y be elements of G .

- (a) Use the uniqueness of inverse elements to prove Proposition 1.2(e): the inverse of the product xy is $y^{-1}x^{-1}$.
- (b) Show that $(x^{-1})^{-1} = x$.

Proposition 1.2(e) can be generalised to the inverse of a product of any number of elements, namely

$$(x_1x_2 \cdots x_n)^{-1} = x_n^{-1} \cdots x_2^{-1}x_1^{-1}.$$

This result is proved by mathematical induction. Even though the proof is not included here, we will use the result when required.

Exercise 1.3

Let G be a group with identity e and let x be an element of G .

- (a) Show that if g is an element of G such that $gx = x$, then $g = e$. In other words, show that if g behaves like a left identity for the particular element x of G , then g is the identity of the group.
- (b) State and prove the corresponding result with ‘left’ replaced by ‘right’.

The solution to Exercise 1.3 provides us with a proof of the following proposition.

Proposition 1.4

Let G be a group with identity e and let x be an element of G .

If g is an element of G such that either $gx = x$ or $xg = x$, then $g = e$.

There is a similar result for inverses: if an element y of a group behaves like a right inverse for another element x , then y is *the* inverse of x .

Proposition 1.5

Let G be a group with identity e and let x be an element of G .

If $xy = e$ for some element y of G , then $y = x^{-1}$.

Proof We are given that $xy = e$. By the inverses axiom, $xx^{-1} = e$. Equating the two expressions for e gives $xy = xx^{-1}$. Using the left cancellation rule, we have $y = x^{-1}$. ■

An alternative proof for Proposition 1.5 involves multiplying both sides of the equation $xy = e$ on the left by the element x^{-1} .

Exercise 1.4

Let G be a group with identity e and let x be an element of G . Show that if an element y of a group G behaves like a left inverse for the element x , that is $yx = e$, then $y = x^{-1}$.

Proposition 1.5 and Exercise 1.4 tell us that if y behaves as either a left inverse or a right inverse of x , then y is *the* inverse of x .

Proposition 1.6

Let G be a group with identity e and let x be an element of G .

If y is an element of G such that either $yx = e$ or $xy = e$, then $y = x^{-1}$.

Before looking at some further examples of groups, we want to say two things about associativity.

Firstly, the associativity axiom guarantees that the two ways of bracketing a combination of *three* elements leads to the same result. It says nothing directly about expressions such as

$$x_1 \circ x_2 \circ \cdots \circ x_n.$$

Fortunately, it is possible to prove (by induction) that all ways of bracketing such an expression lead to the same result. The proof is more involved than illuminating, and so we do not give it. We will assume the result and write such expressions without brackets, doing any specific calculation by combining pairs in the most convenient way.

Proposition 1.7 Generalised associativity rule

Let G be a group and n be a positive integer. Then the product of n elements of G , *taken in a fixed order*, is the same no matter which way the product is calculated.

Secondly, a ‘first principles’ proof that associativity holds in a particular example is usually the messiest part of verifying that an example is a group. Fortunately, for very large classes of groups, including most of those considered in this module, there are quicker ways to prove associativity.

For example, the 2×2 matrices in $\text{GL}(2, \mathbb{R})$ can be thought of as functions from the plane $\mathbb{R}^2$ to itself. The group operation in this case is, effectively, composition of functions. Now, as you may remember from your previous studies, composition of functions is always associative. This fact removes the need to check associativity in any example where the elements are

matrices and the operation is matrix multiplication. We will use this principle freely in the rest of the module.

We can further reduce the number of cases where a check is necessary by observing that if an operation on a given set is associative, then associativity is inherited by any subset that is closed under the operation.

1.2 Permutations

An important example of a whole class of groups is provided by the **symmetric groups** S_n , where n is a positive integer.

The set S_n is defined as the set of all functions

$$f : \{1, \dots, n\} \rightarrow \{1, \dots, n\}$$

where f is a *bijection*, with composition of functions as the operation. The elements of S_n are called **permutations**, and each S_n is an example of a **permutation group**.

We remind you of the notation used for permutations by giving a specific example. In S_4 , the **two-line notation**

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

represents the permutation

$$\begin{array}{lcl} 1 & \mapsto & 4 \\ 2 & \mapsto & 3 \\ 3 & \mapsto & 2 \\ 4 & \mapsto & 1. \end{array}$$

For this permutation, $1 \mapsto 4 \mapsto 1$ and $2 \mapsto 3 \mapsto 2$, so the permutation can be written in **cycles** as

$$(14)(23).$$

The cycles (14) and (23) are **disjoint**, that is, they contain no numbers in common. Any permutation can be broken down into disjoint cycles. A permutation written as a composite of disjoint cycles is said to be in **cycle form**.

Moreover, any cycle $(a_1 a_2 \dots a_n)$ can be expressed as a composite of cycles of length 2 (also called **transpositions**), as follows:

$$(a_1 a_2 \dots a_n) = (a_1 a_n)(a_1 a_{n-1})(a_1 a_{n-2}) \cdots (a_1 a_3)(a_1 a_2).$$

It follows that any permutation can be expressed as a composite of transpositions. This may be done in several different ways, but for a given permutation the number of transpositions appearing in a decomposition is always either even or odd. Thus, a permutation is said to be **even** if it can be expressed as the composite of an even number of transpositions, and **odd** otherwise.

We will often refer to the composition of permutations as a *product*; that is, we will speak about the product of two cycles, or the product of two permutations, to mean their composition.

A bijection is also known as a **one-one correspondence**.

Exercise 1.5

- (a) Evaluate the following product in S_5 , leaving your answer in two-line notation.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 2 & 4 \end{pmatrix}$$

Hint: remember that the permutation on the right must be applied first.

- (b) Write the following element of S_5 in cycle form.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix}$$

- (c) Write the following product in S_6 in cycle form.

$$(163)(254)(13562)$$

Another class of permutation groups are the **alternating groups** A_n , where n is a positive integer. The elements of A_n are all the even permutations in S_n .

1.3 Symmetries of figures

A rich collection of examples of groups comes from considering symmetries of geometric objects. The first example of these that we will consider is shown in Figure 1.1. This group consists of the isometries of the plane that leave the rectangle fixed as a whole; that is, those isometries that map the set of points forming the rectangle onto itself, where we regard a rectangle as consisting of just its boundary. Note that we have not said the isometries fix each point of the rectangle. For example, the isometry given by a half-turn (i.e. a turn through π , denoted by r_π in Figure 1.1) about the centre O of the rectangle leaves no point of the rectangle in its original position (except O itself), but it does fix the whole rectangle and so is a symmetry of the rectangle.

Although you are probably familiar with the symmetries of the rectangle, it will be useful to recall how we can be sure exactly which isometries belong to this group. To do so, we use an approach that will be useful in more complicated examples. The approach is based on certain consequences of the defining property of isometries: that they preserve distance.

We find all the symmetries of the rectangle in two stages. Firstly, we decide what isometries might possibly occur as symmetries. Secondly, we show that all such possibilities are realised.

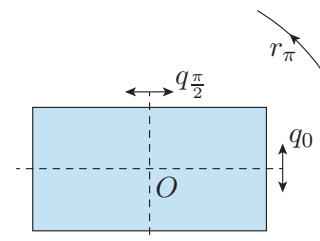


Figure 1.1 Symmetries of a rectangle

The strategy adopted here is a very useful one. We find an upper limit to the number of isometries in a symmetry group and then show that we can find that many different symmetries.

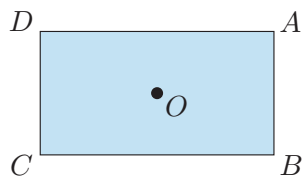


Figure 1.2 Rectangle with labelled corners

The *Cayley table* for a group is a table describing the result of applying the group operation to every pair of elements of the group.

Label the corners of the rectangle A, B, C, D as in Figure 1.2. An isometry must map the corner A to itself or one of the other three corners. Once the image of A is fixed, it must be opposite to the image of C under the isometry. Moreover, since the rectangle is not square and an isometry preserves distances, the image of B must be at the other end of the shorter side from the image of A . Thus the choice of where A maps to determines the isometry. Therefore there are at most four symmetries.

We can indeed find four different symmetries of the rectangle. The identity mapping is one, with A mapping to A ; a half-turn about the point O , with A mapping to C , is another; reflection in the horizontal axis of symmetry, with A mapping to B , gives a third; reflection in the vertical axis of symmetry, with A mapping to D , gives the last. These are all different since A maps to a different corner in each case. Since we know that there are at most four symmetries, we know that we have them all.

If we denote the symmetries (in the order described above) as e, r, h and v , then we can construct a Cayley table where the operation is composition of the symmetries.

$\circ$	e	r	h	v
e	e	r	h	v
r	r	e	v	h
h	h	v	e	r
v	v	h	r	e

By choosing an origin at the centre of the rectangle and coordinate axes parallel to the sides of the rectangle, we can represent the four symmetries e, r, h and v using the following functions from $\mathbb{R}^2$ to $\mathbb{R}^2$:

$$\begin{aligned} e((x, y)) &= (x, y), \\ r((x, y)) &= (-x, -y), \\ h((x, y)) &= (x, -y), \\ v((x, y)) &= (-x, y). \end{aligned}$$

The functions e, r, h and v in turn can be represented by the matrices

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$$

respectively. Thus we have a second representation of the group of symmetries of the rectangle, this time as a group of matrices under multiplication.

There is a third representation of this group, which can be obtained if we number the corners of the rectangle 1 to 4, as in Figure 1.3. Since corners map to corners, each symmetry corresponds to a permutation of the set $\{1, 2, 3, 4\}$, that is to an element of S_4 , as follows:

$$\begin{aligned} e &\text{ corresponds to } \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \\ r &\text{ corresponds to } \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = (13)(24), \\ h &\text{ corresponds to } \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = (12)(34), \\ v &\text{ corresponds to } \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = (14)(23). \end{aligned}$$

These three representations illustrate an important point: a group may have several different but equivalent representations. Here, then, we can consider that we have three concrete examples of groups all essentially the same as the group of symmetries of a rectangle. Thus, depending on the context, we may regard any one of these groups as *the* group of symmetries of a rectangle. The sense in which these representations are ‘equivalent’ and the groups are ‘essentially the same’ will be made more precise in Section 4.

More generally, if we have a subset X of the plane, $\mathbb{R}^2$, then the isometries of $\mathbb{R}^2$ that map X onto itself form a group called the **symmetry group** of X . We will denote the symmetry group of X by $\Gamma(X)$. Thus we denote the **symmetry group of a rectangle** by $\Gamma(\square)$. Where the subset X is large, or complicated, the $\Gamma(\cdot)$ notation can become unwieldy, and in such cases we introduce more convenient notation.

The group of all symmetries of the plane $\mathbb{R}^2$, that is where $X = \mathbb{R}^2$, is known as the **orthogonal group** and denoted by $O(2, \mathbb{R})$. Elements of $O(2, \mathbb{R})$ can be represented by certain 2×2 real matrices with determinant ± 1 . The group of all rotations of the plane, whose elements can be represented by certain 2×2 real matrices with determinant 1, is known as the **special orthogonal group** and denoted by $SO(2, \mathbb{R})$.

The symmetries of a regular hexagon form a group known as the **symmetry group of the regular hexagon**, which we will refer to as D_6 . You may have already met this group in your previous studies under the rather more suggestive names of $\Gamma(\hexagon)$ and $S(\text{Hexagon})$. However, there are two other names in fairly common use. One is our preferred notation D_6 , where the suffix denotes the number of *sides* of the *polygon*; the other is D_{12} , where the suffix indicates the number of *elements* in the *group*. The label D is for *dihedral*. There is a whole family of dihedral groups, one for each regular polygon. You have probably also met D_4 , the **symmetry group of a square**, perhaps with the name $S(\square)$ or $\Gamma(\square)$.

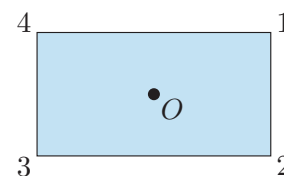


Figure 1.3 Rectangle with numbered corners

This group of four permutations forms a *subgroup* of S_4 , which itself has 24 elements.

Or, more generally still, $\mathbb{R}^n$.

In both cases the group operation is matrix multiplication.

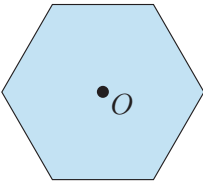


Figure 1.4 A regular hexagon with centre O

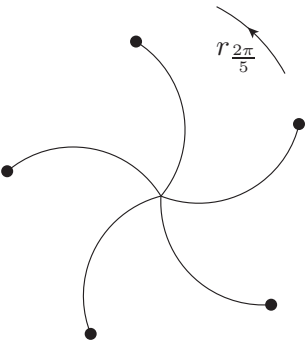


Figure 1.5 A figure whose symmetries give a cyclic group

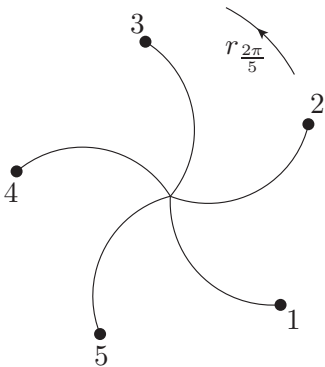


Figure 1.6 Representing rotations as permutations

Exercise 1.6

- (a) Explain why there are at most 12 symmetries of a regular hexagon (Figure 1.4) and how all 12 can be realised.
- (b) In D_6 let r denote anticlockwise rotation through $\frac{\pi}{3}$ and s denote a reflection in an axis of symmetry. Show that $r^6 = e$ and $sr = r^5s$.

Equalities that hold among elements of a group, such as the ones you found in Exercise 1.6(b), are known as **relations**.

1.4 Cyclic groups

Cyclic groups can be regarded as groups of symmetries of figures such as the one shown in Figure 1.5, where we use the curved ‘arms’ to remove any reflections.

Definition 1.8 *Cyclic group*

A group G is **cyclic** if every element has the form g^n for some element g in G . Such an element g is called a **generator** of the group.

A generator for the group of symmetries of the figure in Figure 1.5 is the anticlockwise rotation of $\frac{2\pi}{5}$ about the centre of the figure, denoted by $r_{\frac{2\pi}{5}}$.

The notation $\langle g \rangle$ represents the cyclic group generated by g .

When we considered the symmetries of a rectangle, we represented the symmetries as a set of permutations by labelling the vertices of the rectangle. We can do the same here: if we label each ‘arm’ in the figure with a number from 1 to 5, we can represent the rotations as permutations (Figure 1.6).

The labelling in Figure 1.6 gives the permutation representation shown in Table 1.1.

Table 1.1 Permutation representation using labelling from Figure 1.6

Rotation	Permutation representation
Rotation through $\frac{2\pi}{5}$	$(1\ 2\ 3\ 4\ 5)$
Rotation through $\frac{4\pi}{5}$	$(1\ 3\ 5\ 2\ 4) = (1\ 2\ 3\ 4\ 5)^2$
Rotation through $\frac{6\pi}{5}$	$(1\ 4\ 2\ 5\ 3) = (1\ 2\ 3\ 4\ 5)^3$
Rotation through $\frac{8\pi}{5}$	$(1\ 5\ 4\ 3\ 2) = (1\ 2\ 3\ 4\ 5)^4$
Rotation through 0	$(1)(2)(3)(4)(5) = e = (1\ 2\ 3\ 4\ 5)^5$

In this representation a generator is $(1\ 2\ 3\ 4\ 5)$. We talk about *a* generator, not *the* generator, because the generator of a cyclic group is not necessarily

unique. For example, if we let $g = r_{\frac{2\pi}{5}}$ then $g^5 = e$, the rotation through zero – that is, the identity of the group – and the symmetries of the figure can be given as $\{g, g^2, g^3, g^4, e\}$. They can also be given as

$$\{g^2, (g^2)^2 = g^4, (g^2)^3 = g, (g^2)^4 = g^3, (g^2)^5 = e\},$$

and so g^2 is also a generator of the group. In other words,

$$\langle r_{\frac{2\pi}{5}} \rangle = \langle r_{\frac{4\pi}{5}} \rangle.$$

Recall that a group is **abelian** if the binary operation is commutative. That is, G is an abelian group if

$$a \circ b = b \circ a, \quad \text{for all } a, b \in G.$$

Cyclic groups are abelian, as you are asked to verify in the next exercise.

The usual rules of indices apply.

The term *abelian* is in honour of the Norwegian mathematician Niels Henrik Abel (1802–1829).

Exercise 1.7

Prove that every cyclic group is abelian.

For an abelian group G , we often write the group operation additively, using $+$, so commutativity is expressed as

$$x + y = y + x \text{ for all } x, y \in G.$$

Before we consider such groups, a few words are in order about notation for groups written additively.

When n is a positive integer, the general symbol x^n means n copies of x combined using the group operation. In additive notation this becomes

$$\overbrace{x + \cdots + x}^{n \text{ copies}},$$

which we write as nx rather than x^n .

When $+$ is used for the group operation, the identity is written as 0 and the inverse of x as $-x$.

1.5 Groups from modular arithmetic

Consider $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ with the binary operation addition modulo 6. It is not difficult to see that this set is closed under this operation, that the operation is associative and that the identity is 0. The inverse of each element $a \in \mathbb{Z}_6$ is the standard representative of $-a \pmod{6}$ and so a member of the set. Hence $\mathbb{Z}_6$ with addition modulo 6 is a group. From now on we will use $+_n$ to represent addition modulo n .

Each element a of $\mathbb{Z}_6$ can be obtained by adding 1 to itself $a - 1$ times – that is, adding a ones together. Thus $\mathbb{Z}_6$ is a cyclic group generated by 1.

More generally, the set $\mathbb{Z}_n$ with addition modulo n forms a group for any integer $n > 1$. For these groups, we use either the notation $\mathbb{Z}_n$ or the

notation $(\mathbb{Z}_n, +_n)$, depending on whether we want to specify the operation. For each $n \in \mathbb{N}$, the group $(\mathbb{Z}_n, +_n)$ is cyclic with generator 1.

Exercise 1.8

Write down all the generators of $\mathbb{Z}_6$.

In the solution to Exercise 1.8, you may have noticed that the generators m of $\mathbb{Z}_6$ are precisely those for which $\text{hcf}(m, 6) = 1$. This is an instance of a general property of the cyclic group $\mathbb{Z}_n$: an element m of $\mathbb{Z}_n$ is a generator if $\text{hcf}(m, n) = 1$.

We can also find some cyclic groups by considering modular *multiplication*, as in the example below. From now on, multiplication modulo n will be denoted by $\times_n$, and the set $\mathbb{Z}_n \setminus \{0\}$ by $\mathbb{Z}_n^*$.

Example 1.9 The cyclic group $(\mathbb{Z}_5^*, \times_5)$

Let $G = \mathbb{Z}_5^* = \{1, 2, 3, 4\}$. Then $(G, \times_5)$ is a cyclic group generated by 2 (or 3).

Closure and associativity follow from the rules of modular multiplication.

The identity is 1.

We see that the inverse of 2 is 3, the inverse of 3 is 2 and 4 is self-inverse:

$$2 \times_5 3 \equiv 1 \text{ since } 2 \times 3 = 6 \equiv 1 \pmod{5},$$

$$4 \times_5 4 \equiv 1 \text{ since } 4 \times 4 = 16 \equiv 1 \pmod{5}.$$

As $2^2 \equiv 4 \pmod{5}$, $2^3 \equiv 3 \pmod{5}$ and $2^4 \equiv 1 \pmod{5}$, the group is cyclic and generated by 2.

It is often the case that $\mathbb{Z}_n^*$ is not a group under modular multiplication, since the operation is not closed. For example, in $\mathbb{Z}_6^*$ we have that $3 \times_6 2 \equiv 0$.

Exercise 1.9

Show that $(\mathbb{Z}_5^*, \times_5)$ is not generated by 4.

The notation $\mathbb{Z}_n \setminus \{0\}$ indicates the set $\mathbb{Z}_n$ without the element 0. This is also sometimes denoted by $\mathbb{Z}_n - \{0\}$.

2 Subgroups and cosets

The concept of a subgroup, which you probably met in your previous studies, arises when a group H is contained within a larger group G in such a way that the group operation on H is induced by that on G . This section revises the definition and main properties of subgroups. It also considers how any subgroup gives rise to a partition of the host group into

blocks called *cosets*, and how this notion is pivotal in the proof of the group-theoretic Lagrange's Theorem, a result on the possible sizes of the subgroups of a group.

2.1 Subgroups

We start this section by reminding you of the definition of a subgroup.

Definition 2.1 Subgroup

A subset H of the underlying set of a group G is a **subgroup** of G if it is itself a group under the group operation of G .

We use the notation

$$H \leq G$$

to denote that H is a subgroup of G .

Since H is a subset of G and the group operation is associative in G , the operation is also associative in H , provided H is closed. Thus, checking the group axioms for a subset H of a group G reduces to the following.

Proposition 2.2 Subgroup conditions

If G is a group with binary operation $\circ$ and H is a subset of the underlying set of G , then H is a subgroup of G (with binary operation $\circ$) if all the following conditions are satisfied.

SG1 Closure For all pairs x, y of elements in H , $x \circ y$ is also in H .

SG2 Identity The identity element e of G is in H .

SG3 Inverses For each element x in H , the inverse element x^{-1} in G is also in H .

In particular, the identity of H is the same as the identity of G and inverses of elements in H are the same as their inverses in G .

We will often refer to conditions SG1, SG2 and SG3 as the *subgroup axioms*.

It is worth observing that in order to check for closure, we need only to check pairs of elements x, y where neither element is equal to the identity. This is because if $x, y \in H$ and $x = e$, then $xy = ey = y \in H$. Similarly, if $y = e$, then $xy = x \in H$.

Exercise 2.1

Prove that the set $H = \{e, (1\ 2\ 3), (1\ 3\ 2)\}$ is a subgroup of the permutation group S_3 .

The following proposition reminds you that in any group there are at least two subgroups.

Proposition 2.3

Let G be a group. Then:

- (a) if e is the identity, then $\{e\}$ is a subgroup of G
- (b) G is a subgroup of G .

Proof The subgroup conditions are satisfied in both cases. ■

The subgroup $\{e\}$ is referred to as the **trivial subgroup**. In some texts, the term **proper subgroup** is used for a subgroup that is not the whole group.

Exercise 2.2

Write down all the subgroups of $\mathbb{Z}_6$.

There are several alternative ways of testing whether a particular subset of a group is a subgroup. The one we give in the following proposition is useful because it is somewhat simpler to apply than checking the three conditions in Proposition 2.2.

Proposition 2.4 Subgroup criterion

Let G be a group and H be a subset of the underlying set of G . Then H is a subgroup of G if, and only if, it satisfies the following two properties:

- (a) H is non-empty
- (b) $x, y \in H$ implies $x^{-1}y \in H$.

Proof We start by proving the ‘if’ part of the statement of the theorem: we are given that H is a non-empty subset of G and that, if x and y are in H , then $x^{-1}y$ is in H . We have to show that H is a subgroup of G ; in other words, that H satisfies the three subgroup axioms. It turns out that the easiest way of proving the axioms is not in the order in which they appear in Proposition 2.2, but as follows.

Identity By property (a), H is non-empty. Therefore there exists some element x in H . By property (b), if x and y are in H , then $x^{-1}y$ is in H . The special case $y = x$ shows that $x^{-1}x = e$ is in H . Thus, H satisfies the identity axiom.

Inverses If x is in H then, by the identity axiom (already verified), both x and e are in H . Then, by property (b), the inverse $x^{-1}e = x^{-1}$ is in H , so H satisfies the inverses axiom.

Closure Let x and y be elements of H . By the inverses axiom (already verified), x^{-1} is an element of H . Therefore x^{-1} and y are both in H . So, by property (b), the product $(x^{-1})^{-1}y = xy$ is in H . Therefore H satisfies the closure axiom.

This concludes the proof of the ‘if’ part of the theorem.

For the ‘only if’ part, we need to prove that if H is a subgroup of G , then H has the two properties (a) and (b). You are asked to prove this in Exercise 2.3 below. ■

Exercise 2.3

Let G be a group and H be a subgroup of G . Prove that H is a non-empty subset of G and that, if x and y are elements of H , then so is $x^{-1}y$.

The following exercise asks you to prove an alternative subgroup criterion.

Exercise 2.4

Let G be a group and H be a subset of the underlying set of G . Prove that H is a subgroup of G if, and only if, it satisfies the following two properties:

- (a) H is non-empty, i.e. $H \neq \emptyset$
- (b) $x, y \in H$ implies $xy^{-1} \in H$.

We now have two alternative tests to use to decide whether a subset of a group is a subgroup. We state them in additive notation before looking at an example.

Proposition 2.5 Subgroup criteria (additive notation)

1. A subset H of a group G , written using additive notation, is a subgroup if, and only if, it satisfies the following conditions:
 - (a) H is non-empty
 - (b) $x, y \in H$ implies $-x + y \in H$.
2. A subset H of an additive group G is a subgroup if, and only if, it satisfies the following conditions:
 - (a) H is non-empty
 - (b) $x, y \in H$ implies $x - y \in H$.

The second subgroup criterion looks more natural for abelian groups with additive notation.

As an example, we use criterion 2 of Proposition 2.5 to prove that $(2\mathbb{Z}, +)$ is a subgroup of the group $(\mathbb{Z}, +)$.

Remember that $2\mathbb{Z} = \{2n : n \in \mathbb{Z}\}$.

Firstly, $2\mathbb{Z}$ is non-empty since, for example, $0 = 2 \times 0$ is in $2\mathbb{Z}$.

Secondly, let x and y be two elements of $2\mathbb{Z}$. By the definition of $2\mathbb{Z}$, there exist integers m and n such that $x = 2m$ and $y = 2n$. So

$$x - y = 2m - 2n = 2(m - n).$$

However, $m - n$ is an element of $\mathbb{Z}$. Therefore $2(m - n)$ is an element of $2\mathbb{Z}$.

This completes the proof.

Exercise 2.5

Let G be a group and let H be a subgroup of G .

- (a) Show that if K is a subgroup of H then K is a subgroup of G .
- (b) Show that if K is a subgroup of G and the underlying set of K is a subset of the underlying set of H , then K is a subgroup of H .

The following result is a further consequence of Proposition 2.4.

Proposition 2.6

Let G be a group and H_1 and H_2 be subgroups of G . Then the intersection $H_1 \cap H_2$ is a subgroup of G , and also a subgroup of both H_1 and H_2 .

Proof Firstly, since H_1 and H_2 are subgroups of G , each contains the identity e of G . Therefore e is an element of $H_1 \cap H_2$, and so $H_1 \cap H_2$ is non-empty.

Secondly, if x and y are in $H_1 \cap H_2$, then x and y must be in both H_1 and H_2 . By Proposition 2.4, the product $x^{-1}y$ is in both H_1 and H_2 . Therefore $x^{-1}y$ is in $H_1 \cap H_2$.

We have verified that the intersection $H_1 \cap H_2$ has the two properties in Proposition 2.4, and so $H_1 \cap H_2 \leq G$.

Since, by definition, $H_1 \cap H_2$ is a subset of both of the subgroups H_1 and H_2 , and since, as we have proved, it is a subgroup of G , Exercise 2.5 gives $H_1 \cap H_2 \leq H_1$ and $H_1 \cap H_2 \leq H_2$. ■

Proposition 2.6 generalises to any non-empty collection of subgroups of a group G . For a finite collection, the proof is almost identical to that above. The result is still true for infinite collections of subgroups, though the proof in this case is a little more complicated because of some notational difficulties. Neither proof is given here, but since we will use this result later, we state it in full generality.

Proposition 2.7

Let G be a group. The intersection of any non-empty collection of subgroups of G is a subgroup both of G and of each of the subgroups in the collection.

A natural question that arises now is whether a union of subgroups of a given group is also a subgroup. The answer is no, as the following exercise shows.

Exercise 2.6

Give an example of a group with two subgroups whose union is not a subgroup.

Hint: consider the group $\mathbb{Z}_6$.

It is a fact of life that intersections are nearly always much nicer than unions. This is because intersections share common properties rather than lumping everything together.

Some, but not all, properties of a group are inherited by its subgroups. Here is an example.

Exercise 2.7

Prove that all subgroups of abelian groups are abelian.

2.2 Cosets and Lagrange's Theorem

In your previous mathematical studies you should have encountered the *cosets* of a subgroup in a given group. We remind you of the definition of a *left coset*.

Definition 2.8 *Left coset*

Let G be a group, H be a subgroup of G and a be an element of G . Then the subset

$$aH = \{ah : h \in H\}$$

is called the **left coset** of H by a .

More generally, for any two subsets A and B of G , the set defined by $AB = \{ab : a \in A, b \in B\}$ is said to be the **product** of A and B . So, with this convention, the left coset aH is defined to be the product $\{a\}H$.

Exercise 2.8

Write down all the left cosets of the subgroup $\{e, (12)\}$ in the permutation group S_3 .

Example 2.9 *Cosets of S_3*

In the solution to Exercise 2.8, with $G = S_3$ and $H = \{e, (12)\}$, we saw that the two left cosets eH and $(12)H$ are the same, as are $(13)H$ and $(123)H$, and indeed $(23)H$ and $(132)H$.

So, for different elements a and b of G , the left cosets aH and bH may turn out to be the same.

Moreover, in this example the union of the distinct cosets $\{e, (12)\}$, $\{(13), (123)\}$ and $\{(23), (132)\}$ is the whole group. The cosets are also disjoint, that is, the intersection of any two is the empty set. Furthermore, each coset has the same number of elements.

These results generalise and lead to Lagrange's Theorem.

The conditions under which two cosets are the same are important in the proof of the group-theoretic Lagrange Theorem, which we will see shortly.

In Example 2.9, a coset aH is equal to H precisely when the element a is in H . The following proposition shows that this result holds in general.

Proposition 2.10

Let G be a group and H be a subgroup of G . Then $aH = H$ if, and only if, a is an element of H .

Proof Assume that a is an element of the subgroup H . We want to prove that $aH = H$.

Firstly we show that $aH \subseteq H$. Let x be an element of aH . Then $x = ah$ for some h in H . Now a and h are elements of H and so, by the closure axiom, $ah = x$ is an element of H . Therefore aH is a subset of H .

Secondly we show that $H \subseteq aH$. Let y be an element of H . We may write $y = a(a^{-1}y)$. Since both a and y are in H , so is $a^{-1}y$, by Proposition 2.4. So $y = a(a^{-1}y)$ is an element of aH . Therefore H is a subset of aH .

Hence $aH = H$.

Conversely, assume that $aH = H$. We need to show that a is an element of H .

Since H is a subgroup, the identity element e is in H , therefore ae is in aH . However, $ae = a$ and $aH = H$, so a is in H . ■

Since $H = eH$, we have proved a result about the equality of the cosets aH and eH . A more general result concerning the equality of cosets is given in the following proposition.

Proposition 2.11

Let G be a group, H be a subgroup of G and a and b be elements of G . Then the left cosets aH and bH are equal if, and only if, $a^{-1}b \in H$.

Proof For the ‘if’ part of the statement, we assume that $a^{-1}b$ is an element of H , so $a^{-1}b = h$ for some h in H . To show that $aH = bH$, we must show that $aH \subseteq bH$ and that $bH \subseteq aH$.

Firstly we show that $aH \subseteq bH$. Let x be an element of aH , so that $x = ah_1$ for some h_1 in H . From $a^{-1}b = h$ we deduce (by multiplying both sides on the left by a and on the right by h^{-1}) that $a = bh^{-1}$, and so $x = bh^{-1}h_1$. But $h^{-1}h_1$ is an element of H , so x is an element of bH . Therefore aH is a subset of bH .

Secondly we show that $bH \subseteq aH$. Let y be an element of bH , so that $y = bh_2$ for some h_2 in H . From $a^{-1}b = h$ we deduce (by multiplying both sides on the left by a) that $b = ah$, and so $y = ah h_2$. But $h h_2$ is an element of H , so y is an element of aH . Therefore bH is a subset of aH .

You are asked to prove the ‘only if’ part of the proposition in Exercise 2.9. ■

Exercise 2.9

Let G be a group, H be a subgroup of G and a, b be elements of G such that $aH = bH$. Prove that $a^{-1}b$ is in H .

Since the statement $aH = bH$ in Proposition 2.11 is symmetric in a and b , we can deduce that, in addition,

$$aH = bH \text{ if, and only if, } b^{-1}a \in H.$$

Moreover, Proposition 2.11 allows us to prove the following useful fact.

Proposition 2.12

Let G be a group, H be a subgroup of G and a and b be elements of G . Then the left cosets aH and bH are either disjoint or equal.

Remember that two sets are *disjoint* if they have no elements in common.

Proof Since the cosets aH and bH are either disjoint or not, it suffices to show that if the left cosets aH and bH are not disjoint, then they are equal.

If aH and bH are not disjoint, there exists some element x that is in both aH and bH .

From the definition of left coset, this means that $x = ah_1$ and $x = bh_2$ for some h_1 and h_2 in H . Therefore $ah_1 = bh_2$. Multiplying on the left by a^{-1} and on the right by h_2^{-1} gives $a^{-1}b = h_1h_2^{-1}$. As $h_1h_2^{-1}$ is an element of H , Proposition 2.11 tells us that $aH = bH$. ■

Some conditions that are equivalent to the equality of two cosets are summarised in the next proposition.

Proposition 2.13

Let G be a group, H be a subgroup of G and a and b be elements of G . Then the following four statements are equivalent:

- (a) $a^{-1}b \in H$
- (b) $aH = bH$
- (c) a and b are in the same left coset
- (d) $b \in aH$.

Proof The equivalence (a) $\Leftrightarrow$ (b) is given by Proposition 2.11.

Since $a \in aH$ and $b \in bH$, if $aH = bH$ then a and b are in the same coset. Conversely, if a and b are in the same coset, Proposition 2.12 gives $aH = bH$. We have established the equivalence (b) $\Leftrightarrow$ (c).

Since $a \in aH$, the equivalence (c) $\Leftrightarrow$ (d) follows from Proposition 2.12.

For (a) $\Rightarrow$ (d), if $a^{-1}b \in H$ then $aH = bH$ by Proposition 2.11, and so $b \in aH$. Moreover, $b \in aH$ implies $aH = bH$, again by Proposition 2.12, and so $a^{-1}b \in H$ by Proposition 2.11. Thus (d) $\Rightarrow$ (a). This concludes the proof. ■

Two sets A and B have the *same number of elements* if, and only if, there is a bijection from A to B . This is true even when the two sets are infinite, as the existence of such a bijection is the definition of ‘having the same number of elements’.

The next exercise asks you to prove that all the cosets of a given subgroup of a group have the same number of elements. This result is pivotal in the proof of Lagrange’s Theorem.

Exercise 2.10

Let G be a group, H be a subgroup of G and a and b be elements of G .

- (a) Prove that the function $f : H \rightarrow aH$

$$h \mapsto ah$$

is a bijection, and hence that the sets H and aH have the same number of elements.

- (b) Deduce that the left cosets aH and bH have the same number of elements.

Notation for functions is defined in detail in Book D, Chapter 13, Section 1.

We need two more definitions before we can state and prove Lagrange's Theorem.

Definition 2.14 *Finite and infinite groups*

A group is **finite** if its underlying set is finite, that is, it has a finite number of elements. If the underlying set is infinite, the group is an **infinite group**.

Definition 2.15 *Order of a group*

The **order** of a finite group G is the number of elements it contains, and it is denoted by $|G|$. An infinite group is said to have **infinite order**.

The notation $|G|$ corresponds to other uses of the modulus sign to denote size.

Recall that a collection of subsets $S_1, S_2, \dots, S_k$ of a set S forms a **partition** of S if their union is the whole of S and every pair is disjoint. In this case, we sometimes also say that $S_1, S_2, \dots, S_k$ *partition* S .

With this in mind, we are ready for Lagrange's Theorem. Note that we have already met a result called 'Lagrange's Theorem' in the context of polynomial congruences: Theorem 4.3 of Chapter 4. Both the theorem in Chapter 4 and Theorem 2.16 below are commonly referred to as 'Lagrange's Theorem', even though they are unrelated results. Mathematicians usually rely on the context to make it clear which of the two they are referring to. In this book, 'Lagrange's Theorem' will always denote the group-theoretic result that we are about to prove.

Theorem 2.16 *Lagrange's Theorem*

Let G be a finite group and H be a subgroup of G . Then the order of H divides the order of G , that is,

$$|H| \text{ divides } |G|.$$

Proof Since G has a finite number of elements, so does H .

Assume that the order of H is m .

Let a be any element of G . Then, since $a = ae$, we have that $a \in aH$. This shows that every element of G belongs to some coset of H . In particular, the union of the cosets of H in G is the whole of G . Moreover, by Proposition 2.12, the distinct left cosets of H are disjoint, hence they form a partition of G .

Assume that there are l such distinct cosets. By Exercise 2.10, we know that each of them has m elements. Then the total number of elements in G is lm , which shows that m divides the order of G . ■

Exercise 2.11

Write down all the subgroups of the permutation group S_3 .

You can use Lagrange's Theorem to solve the following exercise.

Exercise 2.12

Let G be a group, and suppose that H and K are two finite subgroups whose orders are coprime. Show that $H \cap K = \{e\}$.

3 Normal subgroups and quotient groups

In the previous section we saw that a subgroup H of a group G partitions G into cosets. This section demonstrates that under certain conditions on H , the set of cosets is itself a group under a suitably defined operation. When the required conditions on H hold, we say that H is a *normal* subgroup, and the group of cosets is called the quotient group.

3.1 Normal subgroups

In the last section we considered only *left* cosets of a subgroup. The concept of *right* coset is entirely similar: given a subgroup H of a group G and an element a of G , we define the **right coset** of H by a as the set

$$Ha = \{ha : h \in H\}.$$

All the results in Subsection 2.2 that hold for left cosets also hold for right ones. For example, we have the following propositions.

Proposition 3.1

Let G be a group, H be a subgroup of G and a and b be elements of G . Then the right cosets Ha and Hb are equal if, and only if, $ab^{-1} \in H$.

The symmetry in a and b implies that an equivalent condition is $ba^{-1} \in H$.

Proposition 3.2

Let G be a group, H be a subgroup of G and a and b be elements of G . Then the right cosets Ha and Hb are either disjoint or equal.

The proofs of these results for right cosets are virtually identical to the ones already given for left cosets, and so we will not write them out.

Given a particular subgroup of a group, it may or may not be the case that a left coset is equal to the corresponding right coset.

Example 3.3 Left and right cosets in S_3

Let $G = S_3$ and $H = \{e, (12)\}$. We saw in Exercise 2.8 that the left coset $(123)H$ is equal to $\{(123), (13)\}$.

On the other hand, the right coset $H(123)$ is

$$\{(123), (12)(123)\} = \{(123), (23)\},$$

which is different from $(123)H$.

However, what is true is that there is a one-one correspondence between the left and right cosets of a given subgroup.

Exercise 3.1

Let G be a group and H be a subgroup of G . Show that the map ϕ from the set of left cosets of H to the set of right cosets of H defined by

$$\phi(aH) = Ha^{-1}, \quad \text{for } a \in G,$$

is well defined, one-one and onto.

ϕ is the Greek letter ‘phi’.

In Exercise 3.1 we have shown the existence of a bijection between the left cosets and the right cosets of a given subgroup. One consequence is that the number of left cosets is the same as the number of right cosets. Thus we can give the following definition.

Definition 3.4 Index of a subgroup

Let G be a group, and H be a subgroup with finitely many cosets. Then the **index** of H in G is the number of left (or right) cosets of H in G .

In the proof of Lagrange's Theorem, we saw that the index of a subgroup H in a finite group G is the quotient $\frac{|G|}{|H|}$. We will make use of this result so often that it is worth highlighting as a proposition.

Proposition 3.5

Let G be a finite group and let H be a subgroup of G . Then the index of H in G is $\frac{|G|}{|H|}$.

Although the number of right cosets of a subgroup is the same as the number of left cosets, we have seen that, in general, if a is an element of G , the left coset aH is different from the right coset Ha . We now consider the special case of a subgroup H where aH and Ha are the same for all $a \in G$.

Definition 3.6 Normal subgroup

Let H be a subgroup of a group G . Then H is a **normal subgroup** of G if

$$aH = Ha$$

for every $a \in G$.

Note that we have *not* said that $ah = ha$ for all $a \in G$ and $h \in H$ individually, but just that the sets aH and Ha are the same.

Exercise 3.2

- Prove that in any group G , the subgroups $\{e\}$ and G are both normal subgroups.
- Prove that all subgroups of an abelian group are normal.

Verifying the normality condition in Definition 3.6 is not usually the most convenient way to check whether a certain subgroup is normal. There are several results of the form

the subgroup H is normal if, and only if, H has some property where the property is easier to check than the definition. Two of these results are given in the following proposition.

Proposition 3.7

Let H be a subgroup of the group G . Then:

- (a) H is a normal subgroup if, and only if, $aHa^{-1} \subseteq H$ for each a in G , where $aHa^{-1} = \{aha^{-1} : h \in H\}$.
- (b) H is a normal subgroup if, and only if, the set of left cosets of H is equal to the set of right cosets of H .

Proof

- (a) Assume that H is a normal subgroup of G . We want to show that $aHa^{-1} \subseteq H$ for each element a of G .

If x is in aHa^{-1} , then $x = ah_1a^{-1}$ for some $h_1 \in H$.

But ah_1 is in aH , which is equal to Ha . Therefore $ah_1 = h_2a$ for some h_2 in H . So

$$x = ah_1a^{-1} = h_2aa^{-1} = h_2 \in H.$$

Therefore $aHa^{-1} \subseteq H$.

Conversely, suppose that $aHa^{-1} \subseteq H$ for each element a of G . We want to show that $aH = Ha$.

We begin by showing that $aH \subseteq Ha$. Let x be in aH , so that $x = ah_1$ for some h_1 in H . The element $xa^{-1} = ah_1a^{-1}$ is in aHa^{-1} . Since aHa^{-1} is a subset of H , it follows that xa^{-1} is in H . Therefore $xa^{-1} = h_2$ for some h_2 in H . Hence $x = h_2a$, which is in Ha , and so aH is a subset of Ha .

We now show that $Ha \subseteq aH$. Let x be in Ha , so that $x = h_1a$ for some h_1 in H . We wish to show that x is in aH , that is, $x = ah$ for some $h \in H$. So we need to show that $a^{-1}x \in H$.

Now $a^{-1}x = a^{-1}h_1a$, and if we rewrite this as

$$a^{-1}h_1a = a^{-1}h_1(a^{-1})^{-1},$$

we see that $a^{-1}x$ is an element of the set $a^{-1}H(a^{-1})^{-1}$.

But the condition $aHa^{-1} \subseteq H$ holds for any $a \in G$, hence also for a^{-1} . So $a^{-1}H(a^{-1})^{-1} = a^{-1}Ha \subseteq H$. Therefore $a^{-1}x = h_2$ for some $h_2 \in H$, and so $x = ah_2$, which is an element of aH . This shows that Ha is a subset of aH . Therefore $aH = Ha$.

- (b) If H is a normal subgroup of G , Definition 3.6 implies immediately that the set of left cosets is equal to the set of right cosets, since $aH = Ha$ for all $a \in G$.

Conversely, assume that the set of left cosets is equal to the set of right cosets. Let $a \in G$ and consider the right coset Ha . By our assumption, $Ha = bH$ for some $b \in G$. Thus $a \in bH$ and we have $bH = aH$ by Proposition 2.13. Thus $Ha = aH$ for all $a \in G$, and so H is normal in G . ■

Exercise 3.3

- (a) Show that $H = \{e, (1\ 2\ 3), (1\ 3\ 2)\}$ is a normal subgroup of the permutation group S_3 .
- (b) Let H be a subgroup of a group G . Prove that if the index of H in G is 2, then H is a normal subgroup.
- (c) Show that the intersection of a collection of normal subgroups of a group G is again a normal subgroup of G .

Given a group G and a subset S of G , there is a unique smallest normal subgroup of G that contains S .

Theorem 3.8

Let G be a group and S be a subset of (the underlying set of) G .

Then there exists a normal subgroup N of G that contains S , and such that for any other normal subgroup M of G containing S , $N \subseteq M$.

Proof Consider the collection of all normal subgroups containing the set S . The collection is non-empty, since G is a normal subgroup containing S . Let N be the intersection of this collection.

By the solution to Exercise 3.3(c), N is a normal subgroup of G . Moreover, N contains S by definition of intersection.

By the method of construction, N is the smallest such normal subgroup. ■

Proposition 3.7(a) might have reminded you about the notion of *conjugacy* in groups. Before giving the key definitions and results concerning conjugacy, we ask you to work through the following exercise.

Exercise 3.4

Let G be a group, H be a subgroup of G and let $g \in G$. Show that the set $gHg^{-1} = \{ghg^{-1} : h \in H\}$ is a subgroup of G .

We are now ready for the definitions of conjugate elements and conjugate subgroups.

Definition 3.9 *Conjugate elements and subgroups*

Let G be a group and let a and b be elements of G .

- (a) The elements a and b are said to be **conjugate elements** in G if there exists $g \in G$ such that $gag^{-1} = b$.
- (b) The **conjugacy class** of a in G is the set of elements conjugate to a , that is, the set

$$\text{Conj}_G(a) = \{gag^{-1} : g \in G\}.$$

- (c) Two subgroups H and K in G are said to be **conjugate subgroups** in G if there exists $g \in G$ such that $gHg^{-1} = K$.

The third part of Definition 3.9 allows us to formulate another criterion to decide whether a given subgroup is normal.

Proposition 3.10

Let G be a group. Then a subgroup N is normal in G if, and only if, N has no conjugate subgroups apart from N .

Proof Let N be normal in G and let $g \in G$. Then $gNg^{-1} \subseteq N$ by Proposition 3.7. Since $N \subseteq gNg^{-1}$, we have $N = gNg^{-1}$ and so N is the only subgroup of G conjugate to N .

Conversely, suppose that N is the only subgroup conjugate to N . Then $gNg^{-1} = N$ for all $g \in G$, so N is normal by Proposition 3.7. ■

The following exercise gives an important property of conjugacy of group elements.

Exercise 3.5

Define a relation $\sim$ on the elements of a group G by

$$a \sim b \text{ if, and only if, } a \text{ is conjugate to } b.$$

Show that $\sim$ is an equivalence relation.

Exercise 3.5 gives some important information on how conjugacy relates to the structure of a group. We describe this relationship more fully in Proposition 3.11.

Proposition 3.11

Let G be a group.

(a) The relation $\sim$ on elements of G defined by

$$a \sim b \text{ if, and only if, } a \text{ is conjugate to } b$$

is an equivalence relation.

(b) The conjugacy classes of G partition the group.

Proof

(a) This is shown in Exercise 3.5.

(b) This follows from part (a), since the equivalence classes of $\sim$ on G are precisely the conjugacy classes. We know that the equivalence classes of an equivalence relation on a set X form a partition of X . We can check this directly for $\sim$ on G as follows.

- Every element of G is conjugate to itself (by reflexivity of $\sim$) and so it belongs to a conjugacy class. Thus the union of the conjugacy classes is G .
- Suppose that an element $c \in G$ belongs to two conjugacy classes $\text{Conj}_G(a)$ and $\text{Conj}_G(b)$ for $a, b \in G$. Then $c \sim a$ and $c \sim b$. By symmetry of $\sim$, we have $a \sim c$, and so $a \sim b$ by transitivity. Thus all the elements of $\text{Conj}_G(b)$ are conjugate to a and vice versa, so

$$\text{Conj}_G(a) = \text{Conj}_G(b).$$

We have shown that two conjugacy classes either are the same or have empty intersection. ■

Exercise 3.6

Write down the conjugacy classes of S_3 .

This exercise might have reminded you that two elements of the group S_n of permutations on n elements are conjugate if, and only if, they have the same cycle type. This is worth remembering when working with symmetric groups.

The conjugacy classes and the normal subgroups of a group G are in fact related, as the following proposition shows.

Proposition 3.12

Let G be a group.

- (a) Any normal subgroup N of G is a union of conjugacy classes.
- (b) Any subgroup H of G that is a union of conjugacy classes is a normal subgroup of G .

Proof

- (a) We claim that N is the union of the conjugacy classes of its elements, namely

$$N = \bigcup_{a \in N} \text{Conj}_G(a).$$

For any $a \in N$ we have $a \in \text{Conj}_G(a)$, so $N \subseteq \bigcup_{a \in N} \text{Conj}_G(a)$.

Now let $a \in N$, and consider any element gag^{-1} of $\text{Conj}_G(a)$. By Proposition 3.7(a), we have $gag^{-1} \in N$. This shows that $\text{Conj}_G(a) \subseteq N$ for any $a \in N$, hence $\bigcup_{a \in N} \text{Conj}_G(a) \subseteq N$.

- (b) Let $h \in H$. Since H is a union of conjugacy classes, there is $a \in G$ such that $h \in \text{Conj}_G(a)$ and $\text{Conj}_G(a) \subseteq H$. Then $h = kak^{-1}$ for some $k \in G$.

Now let $g \in G$. Then

$$ghg^{-1} = g(kak^{-1})g^{-1} = (gk)a(gk)^{-1} \in \text{Conj}_G(a).$$

Since $\text{Conj}_G(a) \subseteq H$, we have that $ghg^{-1} \in H$. Therefore $gHg^{-1} \subseteq H$ for all $g \in G$. By Proposition 3.7(a), H is a normal subgroup of G . ■

3.2 Quotient groups

From the previous section we know that the cosets of a subgroup H of a group G form a partition of G . When H is a normal subgroup, we can say more: we may define a binary operation on the set of cosets of H that makes the set of cosets into a group.

The set of left cosets of a normal subgroup N in G is denoted by G/N . The symbol G/N is read either as ‘the quotient of G by N ’ or, for reasons we will explain shortly, as ‘ G mod N ’.

The binary operation that makes G/N into a group is defined as follows.

From here on in this module, when we refer to a coset of a subgroup we mean a *left* coset, unless otherwise specified.

Definition 3.13 Product of cosets

Let G be a group, N be a normal subgroup of G and let $a, b \in G$. We define the **product** of the cosets aN and bN to be

$$(aN)(bN) = (ab)N.$$

Our definition ensures that the product of two cosets of N is a coset of N . But is this coset unique, that is, is the product of cosets a *well-defined* operation? For example, as we have already seen, it is quite possible for $aN = a_1N$ and $bN = b_1N$ for some elements a_1 and b_1 different from a and b . If this is the case, the product $(aN)(bN) = (a_1N)(b_1N)$ has been defined to be both $(ab)N$ and $(a_1b_1)N$. So our definition will produce a well-defined binary operation only if each such product is uniquely defined, that is, if $(ab)N = (a_1b_1)N$.

The following theorem proves that the product in Definition 3.13 is well defined.

Theorem 3.14

Let G be a group, N be a normal subgroup of G and a, a_1, b and b_1 be elements of G such that

$$aN = a_1N \quad \text{and} \quad bN = b_1N.$$

Then

$$(ab)N = (a_1b_1)N.$$

Proof By Proposition 2.11, to show that $(ab)N = (a_1b_1)N$ it is enough to show that $(ab)^{-1}(a_1b_1)$ is in N .

$$\text{Now, } (ab)^{-1}a_1b_1 = b^{-1}a^{-1}a_1b_1.$$

Since $aN = a_1N$, Proposition 2.11 tells us that $a^{-1}a_1 \in N$, and therefore $b^{-1}a^{-1}a_1 \in b^{-1}N$.

But N is normal, so $b^{-1}N = Nb^{-1}$ and therefore $b^{-1}a^{-1}a_1 = nb^{-1}$, for some n in N . So $(ab)^{-1}a_1b_1 = nb^{-1}b_1$ with n in N .

But Proposition 2.11 also tells us that $b^{-1}b_1 \in N$, and so $(ab)^{-1}a_1b_1$ is a product of two elements of N , namely n and $b^{-1}b_1$. Since N is a group, it follows that $(ab)^{-1}a_1b_1 \in N$. ■

Theorem 3.14 is the first step in proving that the set of cosets G/N , with binary operation defined by $(aN)(bN) = (ab)N$, is a group. In future we will often write $aNbN$ instead of $(aN)(bN)$, and abN instead of $(ab)N$.

All we now need to do is check that the group axioms are satisfied.

The closure axiom is satisfied since, as we remarked above, $(ab)N \in G/N$.

Exercise 3.7

- (a) Check that the binary operation we have defined on the set of cosets G/N is associative.
- (b) Prove that the coset $N (= eN)$ is the identity of G/N .
- (c) Prove that the inverse of the coset aN in G/N is $a^{-1}N$.

The results in Theorem 3.14 and Exercise 3.7 enable us to give the following definition.

Definition 3.15 *Quotient group*

Let N be a normal subgroup of the group G . The **quotient group of G with respect to N** is defined as the group whose underlying set is G/N and whose operation is given by

$$(aN)(bN) = (ab)N \text{ for any } aN, bN \in G/N.$$

Since aN and bN are both subsets of G , we could have defined their product $(aN)(bN)$ as the product of subsets; that is,

$$(aN)(bN) = \{xy : x \in aN, y \in bN\}.$$

This definition has the advantage that the product is well defined, since it depends on the cosets as a whole rather than on the particular elements a and b in the cosets. On the other hand, with this definition it is not immediately clear whether or not the product of two cosets is itself a coset of N . In fact, this definition *does* produce the same product as Definition 3.13, as you will find out in the following exercise.

Exercise 3.8

Prove that if N is a normal subgroup of a group G then

$$\{xy : x \in aN, y \in bN\} = \{(ab)n : n \in N\}.$$

Since $\{(ab)n : n \in N\} = (ab)N$, Exercise 3.8 does indeed show that the two products of cosets defined in this subsection are in fact the same.

In the following exercise you can find out what happens when you attempt to multiply two cosets of a subgroup that is not normal.

Exercise 3.9

Let $G = S_3$ be the group of permutations on three elements and let $H = \{e, (12)\}$.

- (a) Write down the left cosets of H .
- (b) Show that multiplication of these cosets, as described in Definition 3.13, is not well defined.

In the following discussion we consider a quotient group G/H of an abelian group G . In additive notation, the left coset of H containing $a \in G$ is written

$$a + H.$$

We will now illustrate the construction of a quotient group of the abelian group $(\mathbb{Z}, +)$. Consider the set

$$N = 4\mathbb{Z} = \{4z : z \in \mathbb{Z}\}.$$

First, N is a subgroup of $(\mathbb{Z}, +)$. The proof is straightforward and is virtually the same as for $2\mathbb{Z}$, which we discussed in Section 2.

Next, since $(\mathbb{Z}, +)$ is abelian, N is normal by Exercise 3.2.

Let us now determine the distinct cosets of N , i.e. the elements of $\mathbb{Z}/N = \mathbb{Z}/4\mathbb{Z}$.

By Proposition 2.11, the cosets $a + N$ and $b + N$ are equal if, and only if, $a + (-b) \in N$ – in other words if, and only if, a and b differ by a multiple of 4. Thus, two elements of $\mathbb{Z}$ are in the same coset if, and only if, they are equal modulo 4.

Therefore, in additive notation the distinct cosets are

$$\begin{aligned} 0 + 4\mathbb{Z} &= \{4z : z \in \mathbb{Z}\} = 4\mathbb{Z}, \\ 1 + 4\mathbb{Z} &= \{1 + 4z : z \in \mathbb{Z}\}, \\ 2 + 4\mathbb{Z} &= \{2 + 4z : z \in \mathbb{Z}\}, \\ 3 + 4\mathbb{Z} &= \{3 + 4z : z \in \mathbb{Z}\}. \end{aligned}$$

It is clear that the sum of the cosets $a + N$ and $b + N$ is determined by the sum of a and b modulo 4.

The language here is often carried over to the general case. This is why the quotient group G/N is often referred to as ‘ $G \bmod N$ ’. Calculations in the quotient group G/N are like those in G , except that the elements of N are treated as if they were the identity. Thus the quotient group is, in some sense, the group we obtain from the group G by regarding each element $n \in N$ as the identity. We will say more about this aspect of quotient groups later in the chapter.

Exercise 3.10

Let $G = S_3$ be the group of permutations on three elements.

- (a) Write down the only proper non-trivial normal subgroup N of S_3 .
- (b) Write out the Cayley table of G/N .

4 Isomorphisms and homomorphisms

This section gives a mathematical definition of the idea that two groups can have the same structure – that is, that they can be isomorphic. It also explores the more general notion of a homomorphism between two groups (that is, a map that preserves the group operation) and the consequences of the existence of such a map: the First Isomorphism Theorem and the Correspondence Theorem.

4.1 Isomorphisms

In this subsection our aim is to determine under what conditions two groups with the same number of elements are ‘essentially the same’ group. The first problem to be solved in answering this question is to define formally what we mean by saying that two groups are ‘essentially the same’. We will define two groups to be ‘essentially the same’ if they are *isomorphic*, a concept that you are likely to have met in your previous mathematical studies. However, we delay the formal definition until we have looked at some examples in detail.

As an example of a group having four elements, consider an abstract group $\{e, a, b, c\}$ with the following Cayley table.

$\circ$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

This group is called the **Klein group**, and often denoted by V .

We have already seen other examples of groups with four elements. First, in Subsection 1.3, we met $\Gamma(\square)$, the group of symmetries of the rectangle, with the following Cayley table.

$\circ$	e	r	h	v
e	e	r	h	v
r	r	e	v	h
h	h	v	e	r
v	v	h	r	e

Then, in Example 1.9, we met the group of non-zero integers with multiplication modulo 5, whose underlying set is $\{1, 2, 3, 4\}$. Here we will denote this group by $(\mathbb{Z}_5^*, \times_5)$; its Cayley table is as follows.

$\times_5$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

In Subsection 1.5 we also met the groups $(\mathbb{Z}_n, +_n)$ of integers modulo n , with underlying set $\{0, 1, \dots, n-1\}$ and addition modulo n for all positive integers n . The special case $n = 4$ gives another group with four elements.

Exercise 4.1

Write out the Cayley table for the group $(\mathbb{Z}_4, +_4)$.

The following exercise asks you to work with D_4 , the group of symmetries of the square.

Exercise 4.2

Consider the subgroup R of the dihedral group D_4 generated by the rotation r about the centre O through an angle of $\frac{\pi}{2}$ anticlockwise. Prove that R has four elements, and write down its Cayley table.

Let us consider our initial question of whether any of these groups of four elements are ‘essentially the same’. The five groups $(V, \circ)$, $(\Gamma(\square), \circ)$, $(\mathbb{Z}_5^*, \times_5)$, $(\mathbb{Z}_4, +_4)$ and $(R, \circ)$ are not identical, since the underlying sets are different and each has a different binary operation. However, the first two, $(V, \circ)$ and $(\Gamma(\square), \circ)$, are essentially the same in that their Cayley tables have the same pattern: the Cayley table for $(V, \circ)$ becomes the Cayley table for $(\Gamma(\square), \circ)$ by replacing a with r , b with h and c with v . Similarly, the Cayley tables of the fourth and fifth groups have the same pattern as one another, as shown below.

$(\mathbb{Z}_4, +_4)$					$(R, \circ)$				
$+_4$	0	1	2	3	$\circ$	e	r	r^2	r^3
0	0	1	2	3	e	e	r	r^2	r^3
1	1	2	3	0	r	r	r^2	r^3	e
2	2	3	0	1	r^2	r^2	r^3	e	r
3	3	0	1	2	r^3	r^3	e	r	r^2

The Cayley table for $(\mathbb{Z}_4, +_4)$ becomes the table for $(R, \circ)$ if we replace $+_4$ with $\circ$, 0 with e , 1 with r , 2 with r^2 and 3 with r^3 .

These replacements in the headings of the Cayley tables define two bijections:

$$\psi : V = \{e, a, b, c\} \rightarrow \Gamma(\square) = \{e, r, h, v\}, \text{ and}$$

$$\phi : \mathbb{Z}_4 = \{0, 1, 2, 3\} \rightarrow R = \{e, r, r^2, r^3\}.$$

ψ is the Greek letter ‘psi’.

In each case, applying the relevant bijection to the body of the first table produces the second table. This means that ψ and ϕ preserve the effect of the binary operations: the image of the combination of elements in the first table in each case is the same as the combination of their images in the second table. For example, in the second case, for all x and y in $\mathbb{Z}_4$ we have

$$\phi(x +_4 y) = \phi(x) \circ \phi(y).$$

This is what we mean when we say that two groups are ‘essentially the same’. When this is the case, the groups are said to be *isomorphic*.

Definition 4.1 Isomorphism of groups

The groups $(G, \circ)$ and $(H, *)$ are **isomorphic** if, and only if, there exists a bijection $\phi : G \rightarrow H$ such that, for all a and b in G , we have

$$\phi(a \circ b) = \phi(a) * \phi(b).$$

Such a bijection is called an **isomorphism** from G to H .

We use the notation $G \cong H$ to denote that G is isomorphic to H .

In multiplicative notation for both groups, the condition in Definition 4.1 becomes

$$\phi(ab) = \phi(a)\phi(b).$$

This is the notation we will use most of the time. Where the binary operation in each group is addition, the corresponding statement is

$$\phi(a + b) = \phi(a) + \phi(b).$$

Exercise 4.3

Prove that the function $\phi : \mathbb{Z} \rightarrow 2\mathbb{Z}$ defined by

$$\phi : n \mapsto 2n$$

defines an isomorphism from $(\mathbb{Z}, +)$ to $(2\mathbb{Z}, +)$.

We proved that $(2\mathbb{Z}, +)$ was a group in Section 2.

In Definition 4.1, we stated the condition ‘ G and H are isomorphic’ in terms of ϕ as ‘ ϕ is an isomorphism from G to H ’. While the first condition is symmetric in G and H , the second is not. However, there is no conflict here, as the following proposition shows.

Proposition 4.2

Let G and H be groups and let ϕ be an isomorphism from G to H . Then ϕ^{-1} is an isomorphism from H to G .

Proof Since ϕ is a bijection, its inverse ϕ^{-1} is a bijection from H to G . We need to prove that for any two elements x and y of the group H , we have

$$\phi^{-1}(xy) = \phi^{-1}(x)\phi^{-1}(y).$$

Since the function ϕ is onto, there exist elements a and b in G such that $\phi(a) = x$ and $\phi(b) = y$ or, to put it another way, $a = \phi^{-1}(x)$ and $b = \phi^{-1}(y)$. Moreover, since ϕ is an isomorphism we have $\phi(ab) = \phi(a)\phi(b)$.

Therefore

$$\phi^{-1}(xy) = \phi^{-1}(\phi(a)\phi(b)) = \phi^{-1}(\phi(ab)) = ab = \phi^{-1}(x)\phi^{-1}(y). \quad \blacksquare$$

Back to our five example groups: so far we have shown that $(V, \circ)$ and $(\Gamma(\square), \circ)$ are isomorphic and that $(\mathbb{Z}_4, +_4)$ and $(R, \circ)$ are isomorphic. Are there any other isomorphisms among the five groups?

We have already seen that $(\mathbb{Z}_5^*, \times_5)$ and $(\mathbb{Z}_4, +_4)$ are both cyclic groups with four elements, so presumably they too are isomorphic. Their Cayley tables, however, do not seem to have the same pattern as one another.

$(\mathbb{Z}_4, +_4)$					$(\mathbb{Z}_5^*, \times_5)$				
$+_4$	0	1	2	3	$\times_5$	1	2	3	4
0	0	1	2	3	1	1	2	3	4
1	1	2	3	0	2	2	4	1	3
2	2	3	0	1	3	3	1	4	2
3	3	0	1	2	4	4	3	2	1

However, this might just mean that in assuming the elements of $\mathbb{Z}_4$ should correspond to the elements of $\mathbb{Z}_5^*$ in the same order as they appear in the headings of the tables, we are considering the wrong function ϕ . So far we have no clue as to how to look for a bijection from the underlying set of $\mathbb{Z}_4$ to that of $\mathbb{Z}_5^*$ that might show the Cayley tables have the same pattern. On the other hand, we have said that two isomorphic groups are ‘essentially the same’, so it should follow that corresponding elements will have the same properties. This is helpful when looking for a suitable bijection: for example, we would expect the identity of one group to correspond to the identity of the other. This is in fact the case.

Theorem 4.3

Let G and H be groups, let e be the identity of G and let ϕ be an isomorphism from G to H . Then $\phi(e)$ is the identity of H .

Proof As e is the identity for the group G , we know that $ea = a$ for any element a in G .

But ϕ is an isomorphism, so this gives $\phi(e)\phi(a) = \phi(a)$. Therefore $\phi(e)$ behaves like a left identity for the element $\phi(a)$ of H , and so it is the identity of H by Proposition 1.4 of this chapter. ■

By the same token, we expect the image of the inverse of an element under an isomorphism to correspond to the inverse of the image.

Exercise 4.4

Let G and H be groups, and let ϕ be an isomorphism from G to H . Let a be an element of G with inverse a^{-1} . Show that the inverse of $\phi(a)$ is $\phi(a^{-1})$, that is,

$$(\phi(a))^{-1} = \phi(a^{-1}).$$

Hint: as in the proof of Proposition 1.4, use one of the results from Section 1.

So now we know that if there is an isomorphism ϕ from $(\mathbb{Z}_4, +_4)$ to $(\mathbb{Z}_5^*, \times_5)$, then the identity in $\mathbb{Z}_4$ must correspond to the identity in $\mathbb{Z}_5^*$, that is $\phi(0) = 1$, and that inverses must correspond to inverses.

In Example 1.9 we showed that $(\mathbb{Z}_5^*, \times_5)$ is a cyclic group by verifying that the element 2 is a generator. If there is an isomorphism ϕ from $(\mathbb{Z}_4, +_4)$ to this group, then surely a generator in one group must correspond to a generator in the other. So we might try letting the generator 1 in $\mathbb{Z}_4$ correspond to the generator 2 in $\mathbb{Z}_5^*$. Since 3 is the inverse of 1 in $\mathbb{Z}_4$ and 3 is the inverse of 2 in $\mathbb{Z}_5^*$, we should have $\phi(3) = 3$. Then ϕ must send 2 in $\mathbb{Z}_4$ to 4 in $\mathbb{Z}_5^*$.

In fact, when we write the Cayley table of $(\mathbb{Z}_5^*, \times_5)$ as

$\times_5$	1	2	4	3
1	1	2	4	3
2	2	4	3	1
4	4	3	1	2
3	3	1	2	4

we find that it does have the same pattern as the Cayley table for $(\mathbb{Z}_4, +_4)$.

So the function $\phi: \mathbb{Z}_4 \rightarrow \mathbb{Z}_5^*$ defined by

$$\phi(0) = 1, \phi(1) = 2, \phi(2) = 4, \phi(3) = 3$$

is an isomorphism from $(\mathbb{Z}_4, +_4)$ to $(\mathbb{Z}_5^*, \times_5)$.

Exercise 4.5

Find another isomorphism from $(\mathbb{Z}_4, +_4)$ to $(\mathbb{Z}_5^*, \times_5)$.

This would follow because the inverse of an isomorphism is an isomorphism, as is the composite of two isomorphisms.

We have seen that $(\mathbb{Z}_4, +_4)$ is isomorphic to $(R, \circ)$ and to $(\mathbb{Z}_5^*, \times_5)$, and we can deduce that $(R, \circ)$ and $(\mathbb{Z}_5^*, \times_5)$ are isomorphic. We have also seen that $(V, \circ)$ and $(\Gamma(\square), \circ)$ are isomorphic. But is there an isomorphism between $(\mathbb{Z}_4, +_4)$ and $(\Gamma(\square), \circ)$, say, in which case we could deduce that all five groups are isomorphic? The answer is no, but how do we go about showing this?

In order to determine whether or not $(\Gamma(\square), \circ)$ is isomorphic to $(\mathbb{Z}_4, +_4)$, we might think we need to consider all possible ways of writing out its Cayley table, and see whether any of the rearrangements has the same pattern as our table for $(\mathbb{Z}_4, +_4)$. Equivalently, we would have to consider all the bijections from $\mathbb{Z}_4$ to $\Gamma(\square)$ and check whether any of these satisfies the isomorphism property.

At first glance this seems to mean checking $4! = 24$ tables, since that is the number of ways of rearranging four elements. We already know that identity elements must correspond and so must inverses, which cuts down the work somewhat. Nevertheless, this method still involves a considerable amount of effort.

For larger groups this approach would be even more laborious, and it is not a practical way to prove or disprove the existence of an isomorphism between large finite groups. For infinite groups this approach is impossible, since there are an infinite number of possible bijections to consider.

Nevertheless, in practice it is often easier to prove that groups are *not* isomorphic than that they *are*. But why, you might well ask, might we want to know that two groups are not isomorphic?

Well, one of the main objectives of this part of the module is to classify certain classes of groups so that groups that are not isomorphic fall into different classes. In particular, we will classify finite abelian groups. That is, we will know what possible structures an abelian group of a given order can have.

Since isomorphic groups are ‘essentially the same’, they, and their corresponding elements, must have identical algebraic properties.

One way we can show that two groups are not isomorphic is to show that the groups have different algebraic properties.

One property of a finite group is its order, that is, the number of elements it has. Thus, one basic way in which two groups might be different is when they have different numbers of elements. In this case there is no bijection from one group to the other, and so the groups cannot be isomorphic. In particular, it is not possible for a finite and an infinite group to be isomorphic.

We use the word ‘algebraic’ here since it is possible for two groups to be isomorphic and yet to have different *geometric* properties. Consider, for example, the group of the symmetries of the rectangle (Subsection 1.3): the subgroup $\{e, r\}$ is isomorphic to the subgroup $\{e, h\}$ even though one contains a rotation and the other a reflection.

However, when two groups have the same number of elements we need to consider properties other than their order to show that they are not isomorphic.

Exercise 4.6

Let G and H be groups, and let ϕ be an isomorphism from G to H .

- (a) Prove that if G is abelian, then so is H .
- (b) Prove that the groups $\mathbb{Z}_6$ and S_3 are not isomorphic.

The solution to Exercise 4.6 provides one consequence of the existence of an isomorphism between two groups: if one of the groups is abelian, then so is the other. There is a corresponding negative result: an abelian group cannot be isomorphic to a non-abelian one.

Another useful property in deciding whether or not groups are isomorphic is the number of elements in the group having a given order. The definition of the *order of an element* is as follows.

Definition 4.4 Order of a group element

Let a be an element of a group G and let e be the identity in G . Then a has **order** n if, and only if, n is the smallest positive integer such that $a^n = e$. If no such positive integer exists, then the element a is said to have **infinite order**.

We use the notation $|a|$ to denote the order of an element a of finite order.

We have now used the word ‘order’ in two senses: in Section 2 we defined the order of a group and here we have defined the order of a group element. These two are consistent: one consequence of Definition 4.4 is that the order of an element is the order of the cyclic subgroup that it generates. If $a \in G$ has order n , then $|\langle a \rangle| = n$. Even the use of the modulus notation is shared.

Proposition 4.5

Let G be a finite group of order n and let $g \in G$. Then the order of g divides n .

Proof Since G is a finite group, g must have finite order, m say. Then g generates a cyclic subgroup $\langle g \rangle$ of G that has order m . By Lagrange’s Theorem, m must divide n . ■

Exercise 4.7

Let G be a group and $g \in G$. Suppose that $g^n = e$ for some $n \in \mathbb{N}$. Show that the order of g is finite and that it divides n .

Hint: use the Division Algorithm (Book A, Chapter 1, Theorem 4.1) to write $n = qm + r$, where $m = |g|$ and $0 \leq r < m$.

Exercise 4.8

Let G be a group of order p where p is a prime. Show that G is cyclic.

Theorem 4.6

Let G and H be groups and let ϕ be an isomorphism from G to H . Then if $a \in G$ has finite order n , so does $\phi(a) \in H$.

Proof Let e be the identity of G , f be the identity of H and m be the order of $\phi(a)$. Since a has order n , we know that $a^n = e$ and so $\phi(a^n) = \phi(e)$. Now, using Theorem 4.3, we can say that

$$(\phi(a))^n = \phi(a^n) = \phi(e) = f.$$

This tells us that $|\phi(a)| \leq |a|$, that is $m \leq n$, as the order of $\phi(a)$ is the *smallest* positive integer power of $\phi(a)$ that produces the identity f .

As $\phi(a)$ has order m , we know that $(\phi(a))^m = f$, so

$$\phi(a^m) = (\phi(a))^m = f = \phi(e).$$

However, ϕ is a one-one function, so this implies that $a^m = e$.

But a has order n and so $n \leq m$, by the minimality of n . Combining this with the fact that $m \leq n$ gives $m = n$, and so the order of a is the same as the order of $\phi(a)$. ■

Exercise 4.9

Let G and H be groups and let ϕ be an isomorphism from G to H . Prove that if the element a of G has infinite order, then so does $\phi(a)$.

Hint: use the fact that ϕ^{-1} is an isomorphism from H to G to show that if $\phi(a)$ has finite order, then so does a .

Finally, Theorem 4.6 enables us to say that the groups $\mathbb{Z}_4$ and $\Gamma(\square)$ are not isomorphic. The group $\mathbb{Z}_4$ has two elements of order 4 (1 and 3), whereas $\Gamma(\square)$ has no elements of order 4 (each of the non-identity elements has order 2). So having two elements of order 4 is a property that one group has and the other does not.

Here we are using that
 $\phi(a^n) = (\phi(a))^n$.
 This is a straightforward
 extension of the property
 $\phi(ab) = \phi(a)\phi(b)$.

Alternatively, we could have shown that these two groups are not isomorphic by remarking that one of them is cyclic whereas the other is not. You might think that is an easier way to get our result, but in essence Theorem 4.6 is one way of showing that this is a correct argument, as the fact that $\mathbb{Z}_4$ has an element of order 4 is equivalent to the fact that it is a cyclic group, and the fact that $\Gamma(\square)$ has no element of order 4 shows that it is not cyclic. We will see, however, that Theorem 4.6 has a wider application than just to cyclic groups.

4.2 Homomorphisms

In Subsection 4.1 we saw that two groups $(G, \circ)$ and $(H, *)$ are isomorphic when there is a bijection $\phi: G \rightarrow H$ such that, for all a and b in G , we have $\phi(a \circ b) = \phi(a) * \phi(b)$.

If we do not require that ϕ should be one-one and onto, we still obtain a significant notion – that of *homomorphism*.

Definition 4.7 Homomorphism

Let $(G, \circ)$ and $(H, *)$ be groups. A function $\phi: G \rightarrow H$ is a **homomorphism** from G to H if, for all a and b in G , we have

$$\phi(a \circ b) = \phi(a) * \phi(b).$$

The property $\phi(a \circ b) = \phi(a) * \phi(b)$ is referred to as the **morphism** or **homomorphism property**.

So isomorphisms are also homomorphisms, but not all homomorphisms are isomorphisms, since a homomorphism is not necessarily one-one or onto.

Example 4.8 A homomorphism that is neither one-one nor onto

Consider the groups $(\mathbb{Z}, +)$ and $(\mathbb{Z}_4, +_4)$ and the function ϕ from $\mathbb{Z}$ to $\mathbb{Z}_4$ defined by

$$\phi(n) = \begin{cases} 0, & \text{if } n \text{ is even,} \\ 2, & \text{if } n \text{ is odd.} \end{cases}$$

We can see that ϕ is neither one-one (since, for example, $\phi(0) = \phi(2) = 0$) nor onto (since, for example, 1 is not in the image set of ϕ).

We claim that ϕ is a homomorphism. To check this, we must check the morphism property – that is, that for all m and n in $\mathbb{Z}$,

$$\phi(m + n) = \phi(m) +_4 \phi(n).$$

Using the definition of ϕ , this can be done by considering four cases, determined by whether m and n are even or odd.

If m and n are both even, so is $m + n$ and therefore

$$\phi(m + n) = 0 = 0 +_4 0 = \phi(m) +_4 \phi(n).$$

If m is odd and n is even, then $m + n$ is odd and therefore

$$\phi(m + n) = 2 = 2 +_4 0 = \phi(m) +_4 \phi(n).$$

If m is even and n is odd, then $m + n$ is odd and therefore

$$\phi(m + n) = 2 = 0 +_4 2 = \phi(m) +_4 \phi(n).$$

If m and n are both odd, then $m + n$ is even and therefore

$$\phi(m + n) = 0 = 2 +_4 2 = \phi(m) +_4 \phi(n).$$

Therefore we have

$$\phi(m + n) = \phi(m) +_4 \phi(n) \text{ for all } m \text{ and } n \text{ in } \mathbb{Z}.$$

Hence ϕ is an example of a homomorphism that is neither one-one nor onto.

As you may recall from your previous mathematical studies, the set of elements that are mapped by a homomorphism to the identity in the codomain is called the *kernel* of the homomorphism.

Definition 4.9 Kernel

Let $\phi : G \rightarrow H$ be a homomorphism and let e be the identity in H . Then the **kernel** of ϕ is the set

$$\text{Ker}(\phi) = \{x \in G : \phi(x) = e\}.$$

In Example 4.8, the kernel of ϕ consists of all those elements of $\mathbb{Z}$ that map to 0, the identity of $\mathbb{Z}_4$. These are the even integers, that is,

$$\text{Ker}(\phi) = 2\mathbb{Z}.$$

Note that $\text{Ker}(\phi)$ is a subgroup of the domain of ϕ .

Definition 4.10 Image

Let $\phi : G \rightarrow H$ be a homomorphism. Then the **image** of ϕ is the set

$$\text{Im}(\phi) = \{h \in H : h = \phi(x) \text{ for some } x \in G\}.$$

In the case of Example 4.8,

$$\text{Im}(\phi) = \{0, 2\},$$

which is a subgroup of the codomain of ϕ .

Exercise 4.10

Consider the function $\phi : \mathbb{Z} \rightarrow \mathbb{Z}$ defined by

$$\phi : n \mapsto 3n.$$

- (a) Show that ϕ is a homomorphism from $(\mathbb{Z}, +)$ to $(\mathbb{Z}, +)$, but it is not an isomorphism.
- (b) Find the kernel of ϕ and show that it is a subgroup of the domain.
- (c) Find the image of ϕ and show that it is a subgroup of the codomain.

The results of the previous exercise generalise, and we can say rather more about the kernel than just that it is a subgroup of the domain.

Theorem 4.11

Let $\phi : G \rightarrow H$ be a homomorphism from G to H . Then:

- (a) The kernel of ϕ is a normal subgroup of G .
- (b) The image of ϕ is a subgroup of H .

Proof We use multiplicative notation throughout and we denote the identities of G and H by e_G and e_H respectively.

- (a) **Closure** If k and l are in $\text{Ker}(\phi)$, then $\phi(k) = \phi(l) = e_H$. Therefore $\phi(kl) = \phi(k)\phi(l) = e_H e_H = e_H$, and so $kl \in \text{Ker}(\phi)$.

Identity In Theorem 4.3 we showed that for any *isomorphism* ϕ from G to H , if e_G is the identity of G then $\phi(e_G)$ is the identity e_H of H . But the proof of Theorem 4.3 only made use of the morphism property in the definition of an isomorphism, and so the result in the theorem holds for homomorphisms too. Thus $e_G \in \text{Ker}(\phi)$.

Inverses From Exercise 4.4 we know that for any *isomorphism* ϕ from G to H , and for any $x \in G$,

$$\phi(x^{-1}) = (\phi(x))^{-1}.$$

But the solution to Exercise 4.4 only made use of the morphism property in the definition of an isomorphism, and so the result in the exercise holds for homomorphisms too. Hence, if $k \in \text{Ker}(\phi)$ then $\phi(k) = e_H$, so $\phi(k^{-1}) = e_H^{-1} = e_H$. Thus $k^{-1} \in \text{Ker}(\phi)$.

Hence $\text{Ker}(\phi)$ is a subgroup of the domain G .

Normality If $a \in G$ and $k \in \text{Ker}(\phi)$, then

$$\begin{aligned} \phi(aka^{-1}) &= \phi(a)\phi(k)\phi(a^{-1}) \\ &= \phi(a)e_H(\phi(a))^{-1} \\ &= \phi(a)(\phi(a))^{-1} \\ &= e_H. \end{aligned}$$

Therefore $aKa^{-1} \subseteq \text{Ker}(\phi)$ for all a in G . So $\text{Ker}(\phi)$ is a normal subgroup of G .

- (b) **Closure** Let g and h be in $\text{Im}(\phi)$. Then there exist a and b in G such that $\phi(a) = g$ and $\phi(b) = h$. Now ab is in G and $\phi(ab) = \phi(a)\phi(b) = gh$, showing that $gh \in \text{Im}(\phi)$.

Identity Since $\phi(e_G) = e_H$, the homomorphism version of Theorem 4.3 implies that $e_H \in \text{Im}(\phi)$.

Inverses If $h \in \text{Im}(\phi)$, then $h = \phi(g)$ for some $g \in G$. Now, by the homomorphism version of Exercise 4.4,

$$\phi(g^{-1}) = (\phi(g))^{-1} = h^{-1}.$$

Therefore, since $g^{-1} \in G$, we have that $h^{-1} \in \text{Im}(\phi)$. ■

In the next exercise you will discover some group properties that are preserved by homomorphisms.

Exercise 4.11

Let G and H be groups and let $\phi: G \rightarrow H$ be a homomorphism.

- (a) Show that if G is abelian, then so is $\phi(G)$, the image of G under ϕ .
 (b) Let g be an element of finite order n in G . Show that $\phi(g)$ has finite order m , where m divides n .

Theorem 4.11 tells us that a homomorphism ϕ from G to H gives rise to a normal subgroup $\text{Ker}(\phi)$ of the domain G . This normal subgroup can be used to define the quotient group $G/\text{Ker}(\phi)$.

We have also seen that ϕ gives rise to a subgroup of the codomain H , namely $\text{Im}(\phi)$.

It turns out that the quotient $G/\text{Ker}(\phi)$ and the image $\text{Im}(\phi)$ are isomorphic. Before giving a proof of this result, we illustrate it by expanding an example considered earlier.

Example 4.12 An isomorphism between $\mathbb{Z}/2\mathbb{Z}$ and $(\{0, 2\}, +_4)$

Let ϕ be the homomorphism from $\mathbb{Z}$ to $\mathbb{Z}_4$ defined in Example 4.8 by

$$\phi(n) = \begin{cases} 0, & \text{if } n \text{ is even,} \\ 2, & \text{if } n \text{ is odd.} \end{cases}$$

In the discussion following Definition 4.9, we found that $\text{Ker}(\phi) = 2\mathbb{Z}$ and $\text{Im} \phi = \{0, 2\}$.

The cosets of $\text{Ker}(\phi) = 2\mathbb{Z}$ are

$$\begin{aligned} 0 + \text{Ker}(\phi) &= 2\mathbb{Z}, & \text{the set of even integers, and} \\ 1 + \text{Ker}(\phi) &= 1 + 2\mathbb{Z}, & \text{the set of odd integers.} \end{aligned}$$

Since both $\mathbb{Z}/\text{Ker}(\phi)$ and $\text{Im}(\phi)$ are cyclic groups of order 2, they are isomorphic. Because isomorphisms take identities to identities, the only possible isomorphism $\psi : \mathbb{Z}/\text{Ker}(\phi) \rightarrow \text{Im}(\phi)$ is given by

$$\begin{cases} \psi(0 + \text{Ker}(\phi)) = 0 = \phi(0), \\ \psi(1 + \text{Ker}(\phi)) = 2 = \phi(1). \end{cases}$$

Thus $\psi(x + \text{Ker}(\phi)) = \phi(x)$ for all $x \in \mathbb{Z}$.

It turns out that the definition of the isomorphism $\psi : \mathbb{Z}/\text{Ker}(\phi) \rightarrow \text{Im}(\phi)$ in Example 4.12 can be extended to the general case.

Theorem 4.13 First Isomorphism Theorem

Let $\phi : G \rightarrow H$ be a homomorphism from the group G to the group H , with kernel K and image I .

Then the function $\psi : G/K \rightarrow I$ defined by

$$\psi : gK \mapsto \phi(g)$$

is an isomorphism.

Proof Firstly, since ψ is defined in terms of a representative g of the coset gK rather than in terms of gK itself, we must check that ψ is well defined.

For this, we need to show that for any two elements a and b in G , if $aK = bK$ then $\psi(aK) = \psi(bK)$, that is $\phi(a) = \phi(b)$.

Suppose $aK = bK$. Then $a^{-1}b \in K$ by Proposition 2.11. Since K is the kernel of ϕ , this implies that $\phi(a^{-1}b) = e_H$, where e_H is the identity of H . So $\phi(a^{-1})\phi(b) = (\phi(a))^{-1}\phi(b) = e_H$. Multiplying both sides by $\phi(a)$ on the left gives $\phi(a) = \phi(b)$, as required.

We use the homomorphism version of Exercise 4.4.

Secondly, we must show that ψ is one-one; that is, that $\psi(aK) = \psi(bK)$ implies $aK = bK$.

Now, by the way ψ is defined, the condition $\psi(aK) = \psi(bK)$ is equivalent to $\phi(a) = \phi(b)$. But if $\phi(a) = \phi(b)$, reversing the above argument gives $\phi(a^{-1}b) = e_H$. This means that $a^{-1}b \in K$, and so $aK = bK$ by Proposition 2.11.

Next, we must show that ψ is onto.

Any element h of I is of the form $\phi(a)$ for some element a of G . Then $h = \psi(aK)$, which shows that ψ is onto.

Lastly, we must show that ψ has the morphism property; that is, we need to check that $\psi(aK bK) = \psi(aK)\psi(bK)$ for all a and b in G . We have

$$\psi(aK bK) = \psi(abK) = \phi(ab) = \phi(a)\phi(b) = \psi(aK)\psi(bK).$$

This concludes the proof of the theorem. ■

Corollary 4.14

Suppose that $\phi: G \rightarrow H$ is a homomorphism from G to H such that

$$\text{Ker}(\phi) = \{e\}.$$

Then ϕ is an isomorphism from G to $\phi(G) = \text{Im}(\phi)$.

Proof This is the First Isomorphism Theorem in the case where $\text{Ker}(\phi) = \{e\}$. ■

Theorem 4.11 says that all kernels of group homomorphisms are normal subgroups of the domain. Our final result in this subsection shows that the converse is also true: every normal subgroup is the kernel of a suitably defined homomorphism. Thus a subgroup is normal if, and only if, it is the kernel of a homomorphism.

We know that when N is a normal subgroup of a group G , the quotient G/N is a group. This quotient will be the codomain for the homomorphism of which N is the kernel. There is a natural association of the elements of G with the cosets of N : each $a \in G$ is associated with the coset aN to which it belongs.

When we formalise these ideas, we obtain the following theorem.

Theorem 4.15

Let N be a normal subgroup of a group G . Then the function ϕ defined by

$$\phi(a) = aN$$

is a homomorphism from G onto the quotient group G/N .

Furthermore, the kernel of ϕ is N .

Proof We start by noting that ϕ is indeed a function from G to G/N by the way it is defined.

We check the morphism property. For any a and b in G , we have

$$\phi(ab) = abN = aNbN = \phi(a)\phi(b).$$

Thus ϕ is a homomorphism from G to G/N .

We now show that ϕ is onto G/N . Any element of G/N is a coset aN for some element a of G . But aN is the image of the element a under ϕ , because we defined $\phi(a) = aN$. Hence the function ϕ is onto.

Finally, we find the kernel of ϕ . The identity element of G/N is N , therefore a is an element of the kernel of ϕ if, and only if, $\phi(a) = N$. Since $\phi(a) = aN$, we have that $a \in \text{Ker}(\phi)$ if, and only if, $aN = N$. But

Proposition 2.10 implies that $aN = N$ if, and only if, $a \in N$. Hence $\text{Ker}(\phi) = N$. ■

The function ϕ in Theorem 4.15 appears so often in applications that it deserves a specific name.

Definition 4.16 *Natural homomorphism*

Let N be a normal subgroup of a group G . Then the homomorphism $\phi : G \rightarrow G/N$ defined by

$$\phi : a \mapsto aN$$

is called the **natural homomorphism** from G onto G/N .

Exercise 4.12

Show that a quotient group of an abelian group is abelian.

4.3 The Correspondence Theorem

In this subsection we describe the relationship between the subgroups of a group G and the subgroups of a quotient of G by a normal subgroup.

More specifically, we will prove that if G is a group and N is a normal subgroup of G , there is a one-one correspondence between the subgroups of G that contain N and the subgroups of the quotient group G/N , and this correspondence preserves normality. This result is known as the *Correspondence Theorem*.

Figure 4.1 illustrates the correspondence.

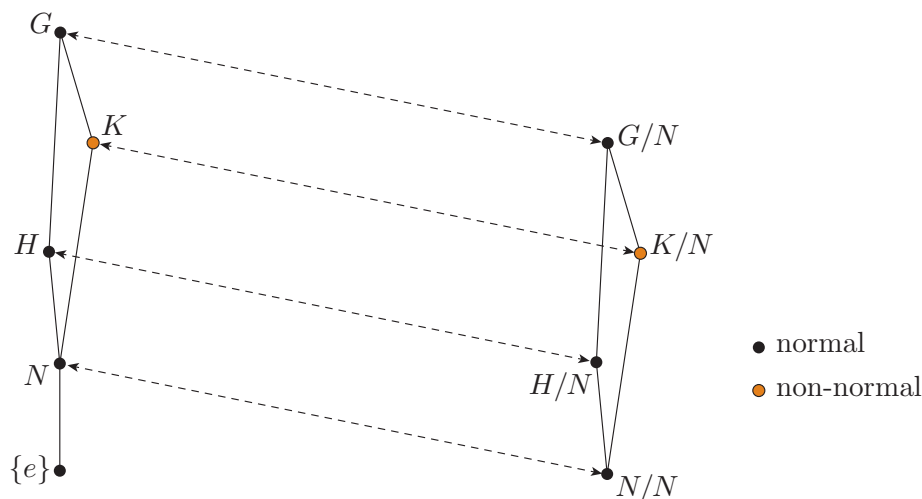


Figure 4.1 Correspondence Theorem

The correspondence can be described in more detail as follows: for any subgroup H of G that contains N , the corresponding subgroup in G/N is H/N . Moreover:

- if H is normal in G then H/N is normal in G/N
- if H is non-normal in G then H/N is non-normal in G/N .

Conversely, if $\overline{H}$ is a subgroup of G/N , then G has exactly one subgroup H that contains N and for which $\overline{H} = H/N$; this subgroup H is the subgroup of G corresponding to $\overline{H}$. Moreover:

- if $\overline{H}$ is normal in G/N then H is normal in G
- if $\overline{H}$ is non-normal in G/N then H is non-normal in G .

In particular, the Correspondence Theorem says that H is normal in G if, and only if, H/N is normal in G/N .

The result you are asked to prove in the following exercise shows you how to determine H from $\overline{H}$, and it will be used in the proof of the theorem.

Exercise 4.13

Observe that H is the set of elements of G that map to an element of $\overline{H}$ under the natural homomorphism.

Let $\overline{H}$ be a subgroup of G/N . Let H be the set defined by

$$H = \{h \in G : hN \in \overline{H}\}.$$

Prove that H is a subgroup of G containing N .

In fact, Exercise 4.13 shows you how to determine the subgroup H of G corresponding to a subgroup $\overline{H}$ of G/N . This will become clearer in the proof of the Correspondence Theorem, which we are now ready for.

Theorem 4.17 Correspondence Theorem

Let G be a group and let N be a normal subgroup of G . Then there is a one-one correspondence between the subgroups of G that contain N and the subgroups of the quotient group G/N . Moreover, this correspondence maps normal subgroups of G to normal subgroups of G/N and vice versa.

Proof Let G and N be as in the statement of the theorem.

Define a map α from the set of subgroups of G that contain N to the set of subgroups of the quotient group G/N by

$$\alpha(H) = \{hN : h \in H\} \text{ for any subgroup } H \text{ of } G \text{ containing } N.$$

Observe that α is related to the natural homomorphism $\phi : G \rightarrow G/N$, in that $\alpha(H)$ is the image of the subgroup H under ϕ . Therefore, by Theorem 4.11 we have that $\alpha(H)$ is a subgroup of G/N . Moreover, from the way α has been defined, it preserves inclusions; that is, if $H \subseteq K$ then $\alpha(H) \subseteq \alpha(K)$.

α is the Greek letter ‘alpha’.

The natural homomorphism ϕ and the map α have different domains and codomains: while ϕ maps elements of G to cosets of N in G , the map α takes subgroups of G to subgroups of G/N .

Our aim is to show that α is one-one and onto and gives the required correspondence.

We start by showing that α is one-one. Suppose that H_1 and H_2 are two subgroups of G containing N such that

$$\alpha(H_1) = \alpha(H_2).$$

Let x_1 be an element of H_1 . By the definition of α , the coset x_1N is an element of $\alpha(H_1) = \alpha(H_2)$. Hence there exists an element x_2 of H_2 such that $x_1N = x_2N$. Therefore, by the condition for the equality of cosets, $x_2^{-1}x_1 \in N$. Now, N is contained in H_2 and so

$$x_2^{-1}x_1 \in H_2.$$

But $x_2 \in H_2$ and so, by closure, $x_2(x_2^{-1}x_1) = x_1 \in H_2$. This shows that $H_1 \subseteq H_2$. All the conditions that we have used in this argument are symmetric in H_1 and H_2 , so if we exchange the subscripts 1 and 2 throughout, we obtain a proof that $H_2 \subseteq H_1$. Hence $H_1 = H_2$ and α is one-one.

To show that α is onto, let $\overline{H}$ be a subgroup of G/N and define $H \subseteq G$ by

$$H = \{h \in G : hN \in \overline{H}\}.$$

Exercise 4.13 ensures that H is a subgroup of G containing N . We claim that $\alpha(H) = \overline{H}$.

Remember that

$$\alpha(H) = \{hN : h \in H\},$$

so from the definition of α we have that $h \in H$ if, and only if, $hN \in \overline{H}$. Hence $\alpha(H) = \overline{H}$, and α is onto.

We have established that α gives a one-one correspondence that is onto and preserves inclusion. We can also deduce from the definition of α that $\alpha(N) = \{N\}$, the trivial subgroup of G/N , and that $\alpha(G) = G/N$, the whole of the quotient group.

We now show that this correspondence sends normal subgroups to normal subgroups.

Firstly, assume that $H \leq G$ is a normal subgroup of G containing N and let $\overline{H} = \alpha(H)$. We want to show that $\overline{H}$ is normal in G/N . Let $x \in \overline{H}$ and $y \in G/N$. Then

$$\begin{aligned} x &= hN && \text{for some } h \in H \text{ and} \\ y &= gN && \text{for some } g \in G. \end{aligned}$$

Since H is normal in G and $h \in H$, we have $ghg^{-1} \in H$.

Hence $yxy^{-1} = (gN)(hN)(gN)^{-1} = (gN)(hN)(g^{-1}N) = (ghg^{-1})N \in \overline{H}$.

This completes the proof that $\overline{H}$ is normal in G/N .

Now assume that $\alpha(H) = \overline{H}$ is a normal subgroup of G/N . Let $h \in H$ and $g \in G$. Then gN is an element of G/N and, by the correspondence, $hN \in \overline{H}$.

By the normality of $\overline{H}$,

$$(gN)(hN)(gN)^{-1} \in \overline{H}.$$

Hence $\overline{H}$ contains $(gN)(hN)(gN)^{-1} = (gN)(hN)(g^{-1}N) = (ghg^{-1})N$.

Since $(ghg^{-1})N \in \overline{H}$, we have $ghg^{-1} \in H$. This completes the proof that H is normal in G . ■

Corollary 4.18

Let G be a group, N be a normal subgroup of G and H be a subgroup of G that contains N . If G is finite, the index of H in G is equal to the index of H/N in G/N ; that is,

$$\frac{|G|}{|H|} = \frac{|G/N|}{|H/N|} = \frac{|\overline{G}|}{|\overline{H}|}.$$

The Correspondence Theorem can be used to investigate the structure of the subgroups of a given group: if N is a proper, non-trivial normal subgroup of a finite group G , then both G/N and N are smaller than G . More generally, G/N and N will be less complex than G , and so finding subgroups of G/N may be easier than finding subgroups of G . The Correspondence Theorem then gives the corresponding subgroups of G .

One consequence of the Correspondence Theorem is that every subgroup $\overline{H}$ of G/N has the form H/N for some $H \leq G$. Exercise 4.13 tells us how to find H from $\overline{H}$: remember that $H = \{h \in G : hN \in \overline{H}\}$, so in fact

$$H = \bigcup_{gN \in \overline{H}} gN,$$

Since N is a normal subgroup of G , its left and right cosets are identical; we therefore refer simply to ‘the cosets’ of N in G .

the union of the cosets of N that belong to $\overline{H}$.

The inclusion $H \subseteq \bigcup_{gN \in \overline{H}} gN$ follows from the definition of H . To see why the reverse inclusion holds, suppose that $h \in gN$ for some coset $gN \in \overline{H}$. Then $h = gn$ for some $n \in N$, so $hN = gnN = gN$ and therefore $h \in H$, as required.

Note also that when H is finite, the number of elements in H is the number of elements in N times the number of elements in $\overline{H}$; that is,

$$|\overline{H}| = \frac{|H|}{|N|} \quad \text{and} \quad |H| = |N| \times |\overline{H}|.$$

5 The group of permutations on four elements

In this section you will work through a series of exercises about the group S_4 . This should consolidate the ideas covered in this chapter.

The first exercise is for you to practise cycle notation for permutations. Remember that we use e to denote the identity permutation.

Exercise 5.1

(a) Express the following products as products of disjoint cycles.

(i) $(1\ 2\ 3)(1\ 2)$

(ii) $(1\ 2\ 3\ 4)(1\ 3)$

(iii) $(1\ 3)(1\ 2\ 3\ 4)$

(iv) $(1\ 2)(1\ 3\ 4\ 2)(1\ 2)$

(v) $(1\ 2\ 3)(1\ 4\ 3\ 2)(1\ 4)$

(b) Write down the inverse of each of the permutations in part (a).

The next exercise asks you to check that certain sets of permutations are subgroups of S_4 . Suppose you are asked to show that

$$H = \{e, (1\ 2\ 3\ 4), (1\ 3)(2\ 4), (1\ 4\ 3\ 2)\}$$

is a subgroup of S_4 . One way to establish closure is to compile the Cayley table of H , and then confirm that H contains the inverse of each of its elements. However, there are simpler methods. For instance, you might spot that H is the cyclic subgroup $\langle (1\ 2\ 3\ 4) \rangle$ of S_4 , so closure is immediate. Alternatively, the elements of H can be realised as the four rotational symmetries of a square whose corners are labelled 1, 2, 3 and 4: we know these symmetries form a group. Still another way is to look at the elements of H as the symmetry group of Figure 5.1.

You may remember from your previous studies the distinction between *direct* and *indirect* symmetries. For our purposes, the direct symmetries of a plane figure are the rotations, whereas the indirect symmetries are the reflections. The set of direct symmetries of any figure forms a group, as does the set of all symmetries.

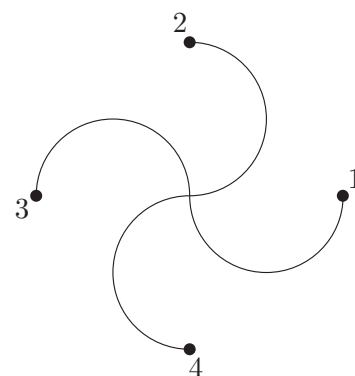


Figure 5.1 Figure whose symmetries give the subgroup $\langle (1\ 2\ 3\ 4) \rangle$ of S_4

Thus, considering the symmetries of a plane figure gives a useful way to find subgroups of permutation groups (as shown in Figure 5.2 for S_4), as the following exercise illustrates.

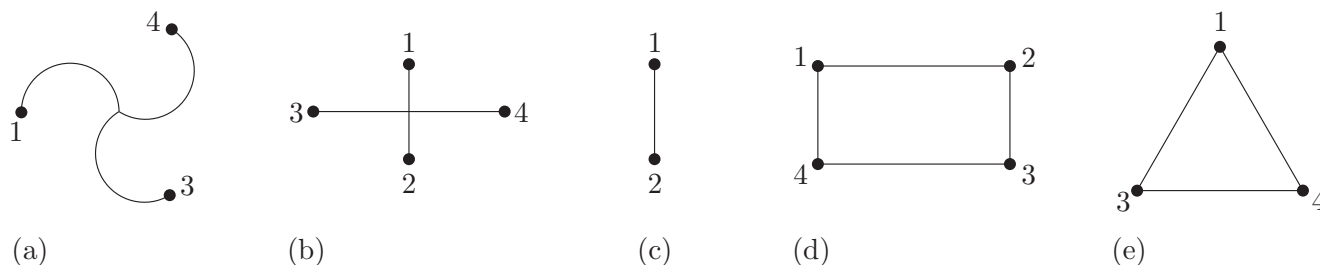


Figure 5.2 Figures whose symmetries give subgroups of S_4

Exercise 5.2

Show that each of the following subsets of S_4 is a group under composition of permutations.

- (i) $H_1 = \{e, (1\ 2)\}$
- (ii) $H_2 = \{e, (1\ 3\ 4), (1\ 4\ 3)\}$
- (iii) $H_3 = \{e, (1\ 3), (1\ 4), (3\ 4), (1\ 3\ 4), (1\ 4\ 3)\}$
- (iv) $H_4 = \{e, (1\ 2), (3\ 4), (1\ 2)(3\ 4)\}$
- (v) $H_5 = \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$

Hint: each of these sets can be related to one of the figures in Figure 5.2.

Another noteworthy example of a symmetry group is $\Gamma(\text{TET})$, the group of symmetries of a regular tetrahedron. This group contains 24 elements:

- the identity
- eight rotations about an axis through a vertex and the opposite face
- three rotations about a line joining opposite edges
- twelve other symmetries – six reflections in the plane through an edge joining two vertices and the midpoint of the edge joining the other two vertices, and six others, each obtained by composing a reflection and a rotation.

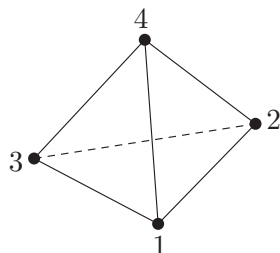


Figure 5.3 A tetrahedron with vertices 1, 2, 3 and 4

If we represent each symmetry by the way in which it permutes the vertices of the tetrahedron (labelled 1, 2, 3 and 4 as in Figure 5.3), we get precisely the elements of S_4 . Thus, the groups $\Gamma(\text{TET})$ and S_4 are isomorphic.

Cosets are much maligned and misunderstood. In fact they often highlight interesting aspects of a group. It is often the case that a set H forms a subgroup of a group G because all the elements of H share a noteworthy property; moreover, the cosets of H partition G in such a way that all the elements in a single coset share a different but closely related property. Here is an example of what we mean.

Example 5.1 Cosets in S_4

We know from Exercise 5.2 that $H_3 = \{e, (1\ 3), (1\ 4), (3\ 4), (1\ 3\ 4), (1\ 4\ 3)\}$ is a subgroup of S_4 . Note also that $H_3 \cong S_3$. However, when H_3 is viewed as a subgroup of S_4 , it is characterised by the property that each of its elements fixes 2.

When we consider the cosets of H_3 in S_4 , we find that:

- every element of $(1\ 2)H_3$ sends 2 to 1
- every element of $(2\ 3)H_3$ sends 2 to 3
- every element of $(2\ 4)H_3$ sends 2 to 4.

So the left cosets of H_3 partition S_4 in an interesting way.

The group H_3 in Example 5.1 is not normal in S_4 , so the set of right cosets of H_3 in S_4 gives a different partition of S_4 .

Exercise 5.3

Let H_3 be as in Exercise 5.2. For each right coset of H_3 in S_4 , work out a property shared by its elements.

Viewing cosets in this way will be useful when you meet *group actions* in Chapter 6, as it will give interesting insights into the link between group actions and homomorphisms.

Now we begin a systematic search for *all* subgroups of S_4 . First we use Lagrange's Theorem to find the possible orders of these subgroups. Then we look at the elements of S_4 and consider their cycle structure and order. Once we have done this, we will be in a position to find and list all the subgroups of S_4 .

Recall that the alternating group A_n is a normal subgroup of S_n and consists of all the even permutations in S_n . In particular, A_4 has order 12.

Exercise 5.4

- What are the possible orders of the subgroups of S_4 ?
- The elements of S_4 have different cycle structures. For each of these cycle structures, write down one element, and the total number of elements with that structure. State the order of the elements of each type.
- Write down the orders of the elements of S_4 , and how many elements there are of each order.

We now examine *conjugacy* in S_4 : two elements g and h of S_4 are conjugate if there exists $k \in S_4$ such that $kgk^{-1} = h$.

We know that two permutations are conjugate in the symmetric group S_n if, and only if, they have the same cycle structure. So, for example, $(1\ 2\ 3)$ and $(1\ 4\ 2)$ are conjugate in S_4 , as are $(1\ 3)(2\ 4)$ and $(1\ 4)(2\ 3)$. However, the permutations $(1\ 3)(2\ 4)$ and $(1\ 2)(2\ 3)$ are not conjugate in S_4 , since $(1\ 2)(2\ 3)$ is not the cycle form of a permutation, because it is not a product of *disjoint* cycles – in fact,

$$(1\ 2)(2\ 3) = (1\ 2\ 3).$$

Recall from Definition 3.9 of this chapter that the conjugacy class of an element g in a group G is the set of elements of G that are conjugate to g .

Exercise 5.5

- (a) Calculate the conjugate hgh^{-1} of g in S_4 , where
 - (i) $g = (1\ 3)$, $h = (1\ 2)(3\ 4)$
 - (ii) $g = (1\ 2\ 3\ 4)$, $h = (1\ 4\ 2)$.
- (b) Find elements g_1 and g_2 in S_4 such that $g_1(1\ 2)g_1^{-1} = (2\ 4)$ and $g_2(1\ 2\ 3\ 4)g_2^{-1} = (1\ 3\ 4\ 2)$.
- (c) How many conjugacy classes are there in S_4 , and how many elements are there in each class?

The following exercise asks you to examine certain subgroups of S_4 .

Exercise 5.6

- (a) How many subgroups of order 2 does S_4 have, and how many of order 3?
- (b) Find all cyclic subgroups of S_4 of order 4.
- (c) The set $V = \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ is a subgroup of S_4 called the *Klein subgroup*, as it is isomorphic to the Klein group, which you met in Subsection 4.1 of this chapter. Is V cyclic? Find all the subgroups of S_4 that are isomorphic to V .
- (d) Why does S_4 not contain any *cyclic* subgroups of order 6?
- (e) In Exercise 5.2 you showed that H_3 is a subgroup of S_4 of order 6. Find three further subgroups of S_4 of order 6.
- (f) By considering the symmetry groups of various plane figures, find a subgroup of S_4 of order 8. Then find two more. Does S_4 contain any cyclic subgroups of order 8?
- (g) Find a subgroup of S_4 of order 12.

Although we are not yet in a position to prove this, in Exercise 5.6 we found all the subgroups of S_4 of orders 2, 3, 4, 6, 8 and 12; that is, all the proper non-trivial subgroups.

Exercise 5.7

Describe in words the groups H_2 and H_3 of Exercise 5.2 and A_4 of Exercise 5.6 as subgroups of $\Gamma(\text{TET})$.

(It is rather more difficult, but interesting, to interpret all the other subgroups of S_4 in terms of the geometry of the tetrahedron.)

Recall from Definition 3.9 of this chapter that two subgroups H and K of G are said to be conjugate in G if there exists $g \in G$ such that $gHg^{-1} = K$.

Exercise 5.8

- (a) Determine the subgroups $(1\ 2)H_3(1\ 2)^{-1}$ and $(1\ 3\ 2\ 4)H_4(1\ 3\ 2\ 4)^{-1}$, where H_3 and H_4 are as in Exercise 5.2.
- (b) Are the subgroups H_4 and H_5 of Exercise 5.2 conjugate in S_4 ?
- (c) Are all subgroups of order 2 conjugate to one another in S_4 ?
- (d) Are all subgroups of order 3 conjugate to one another in S_4 ?

Exercise 5.9

Deduce from Proposition 3.12 and Exercise 5.4 that the only possible orders for non-trivial proper normal subgroups of S_4 are 4 and 12.

Confirm that normal subgroups of S_4 with orders 4 and 12 do indeed exist.

In Subsection 4.2 we saw that there is a correspondence between normal subgroups and kernels of group homomorphisms, in that the kernel of a homomorphism is a normal subgroup of the domain and, conversely, every normal subgroup of a group G is the kernel of some homomorphism with domain G .

Now you are asked to work with the important subgroup A_4 of S_4 .

Exercise 5.10

- (a) Recall that A_4 is a normal subgroup of S_4 . If a homomorphism has domain S_4 and kernel A_4 , how large is its image set?
- (b) Write down a homomorphism whose domain is S_4 and whose kernel is A_4 .

Hint: try a map with codomain $\mathbb{Z}_2$.

Exercise 5.11

- (a) What are the possible orders of subgroups of A_4 ?
- (b) Find all the subgroups of A_4 and give their orders. Does A_4 have a subgroup of order 6? What is the significance of this result?
- (c) Are the elements $(1\ 2\ 3)$ and $(2\ 3\ 4)$ conjugate in A_4 ? (Careful!)
- (d) Find the conjugacy classes in A_4 of elements of A_4 .
- (e) Find all non-trivial proper normal subgroups of A_4 .

Exercise 5.12

Use your results from this section to complete the following table.

	S_4	A_4
(a) order of group		
(b) number of subgroups of order 2		
(c) number of subgroups of order 3		
(d) number of cyclic subgroups of order 4		
(e) number of non-cyclic subgroups of order 4		
(f) number of cyclic subgroups of order 6		
(g) number of non-cyclic subgroups of order 6		
(h) number of subgroups of order 8		
(i) number of subgroups of order 12		
(j) total number of subgroups		
(k) total number of normal subgroups		

Exercise 5.13

Show the relations given by the Correspondence Theorem between S_4 , with its normal subgroups A_4 and V , and the quotient group S_4/V in a diagram similar to that in Figure 4.1.

Learning outcomes

We list those topics on which we may set assessment questions to test your understanding of the chapter.

After working through this chapter you should be able to:

- (a) Use the group axioms to check whether a given set with a specified binary operation is a group.
- (b) Check whether a given subset of a group is a subgroup.
- (c) Obtain the symmetry groups of simple geometric figures.
- (d) Decide whether a group is cyclic.
- (e) Partition a group into cosets of a given subgroup.
- (f) Check whether a given subgroup of a group is normal.
- (g) Form and identify quotient groups in simple cases.
- (h) Check whether a given function between two groups is an isomorphism or a homomorphism.
- (i) Decide whether two given groups are isomorphic.
- (j) Find kernels and images of group homomorphisms.
- (k) Compute products and conjugates of permutations.
- (l) Construct proofs, similar to those in the chapter, based on the group axioms and the results of the chapter.
- (m) Recognise familiar examples such as the Klein group, the cyclic groups $\mathbb{Z}_n$, the symmetry groups S_n and the alternating group A_4 .

Solutions to exercises

Solution to Exercise 1.1

We need to check that the group axioms hold in each case. Since we are told we can assume associativity for matrix multiplication, we need only to check the other three axioms.

- (a) **Closure** If $\mathbf{A}$ and $\mathbf{B}$ are two 2×2 matrices with real entries, the process of matrix multiplication guarantees that the product $\mathbf{AB}$ is 2×2 with real entries. This is not enough: we also need that the determinant of $\mathbf{AB}$ is non-zero. Recall that for any 2×2 matrices $\mathbf{A}$ and $\mathbf{B}$,

$$\det(\mathbf{AB}) = \det(\mathbf{A}) \det(\mathbf{B})$$

(a proof of this result is reproduced below for completeness).

Therefore if $\mathbf{A}$ and $\mathbf{B}$ both have non-zero determinants, so has $\mathbf{AB}$.

This completes the closure argument.

To see that $\det(\mathbf{AB}) = \det(\mathbf{A}) \det(\mathbf{B})$, let

$$\mathbf{A} = \begin{bmatrix} a & c \\ b & d \end{bmatrix} \quad \text{and} \quad \mathbf{B} = \begin{bmatrix} e & g \\ f & h \end{bmatrix}.$$

Then $\mathbf{AB} = \begin{bmatrix} ae + cf & ag + ch \\ be + df & bg + dh \end{bmatrix}$ and so

$$\begin{aligned} \det(\mathbf{AB}) &= (ae + cf)(bg + dh) - (ag + ch)(be + df) \\ &= aebg + aedh + cfbg + cfdh - agbe - agdf - chbe - chdf \\ &= aedh + cfbg - agdf - chbe \\ &= ad(eh - gf) - bc(eh - gf) \\ &= (ad - bc)(eh - gf) \\ &= \det(\mathbf{A}) \det(\mathbf{B}). \end{aligned}$$

Identity The matrix $\mathbf{I} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ acts as an identity for matrix multiplication and has determinant 1, which is non-zero.

Inverses If $\mathbf{A} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ and $\det(\mathbf{A}) = ad - bc \neq 0$, then

$$\mathbf{A}^{-1} = \frac{1}{ad - bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}.$$

Then $\mathbf{A}^{-1}$ has real entries. Moreover,

$$\det(\mathbf{A}) \det(\mathbf{A}^{-1}) = \det(\mathbf{AA}^{-1}) = \det(\mathbf{I}) = 1,$$

so $\mathbf{A}^{-1}$ has non-zero determinant.

- (b) **Closure** We take two typical elements and show that the product is of the right form to be in the specified set. So, suppose that a, b are in $\mathbb{Z}$. Then

$$\begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a+b \\ 0 & 1 \end{bmatrix}.$$

Since $a+b$ is also in $\mathbb{Z}$, the product of the two matrices is also in the set. This proves closure.

Identity The matrix $\mathbf{I} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ acts as an identity for matrix multiplication. We need to check that it belongs to the set in question. Since the leading diagonal elements are 1, the bottom left element is 0 and the top right element is an integer (namely 0), $\mathbf{I}$ is in the set.

Inverses A typical element of the given set has the form $\begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}$ and has determinant $1 \neq 0$, so it has a multiplicative inverse. We need to check that the inverse belongs to the specified set. We have

$$\begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}^{-1} = \begin{bmatrix} 1 & -a \\ 0 & 1 \end{bmatrix}.$$

Since $-a$ is an integer whenever a is, the inverse matrix has the required form and does indeed belong to the set.

Solution to Exercise 1.2

- (a) We need to verify that $y^{-1}x^{-1}$ has the defining property of the inverse of xy , that is,

$$(xy)(y^{-1}x^{-1}) = e = (y^{-1}x^{-1})(xy).$$

Now

$$\begin{aligned} (xy)(y^{-1}x^{-1}) &= (x((yy^{-1})x^{-1})) && \text{(Associativity)} \\ &= x(ex^{-1}) && \text{(Identity)} \\ &= xx^{-1} && \text{(Identity)} \\ &= e, && \text{(Identity)} \end{aligned}$$

so $y^{-1}x^{-1}$ behaves as a *right* inverse for xy . Moreover,

$$\begin{aligned} (y^{-1}x^{-1})(xy) &= y^{-1}((x^{-1}x)y) && \text{(Associativity)} \\ &= y^{-1}(ey) && \text{(Identity)} \\ &= y^{-1}y && \text{(Identity)} \\ &= e. && \text{(Identity)} \end{aligned}$$

So $y^{-1}x^{-1}$ also behaves as a *left* inverse for xy .

Hence, by the uniqueness of inverses, $y^{-1}x^{-1}$ is the inverse of xy .

- (b) We give a proof that uses the cancellation rules.

Because $(x^{-1})^{-1}$ is the inverse of x^{-1} , we have

$$x^{-1} (x^{-1})^{-1} = e.$$

On the other hand, x^{-1} is the inverse of x , and so $x^{-1}x = e$.

Equating the two expressions for e gives $x^{-1} (x^{-1})^{-1} = x^{-1}x$, and left cancellation gives the desired result.

Solution to Exercise 1.3

- (a) We are given that $gx = x$ and, by the identity axiom, we know that $ex = x$.

Hence $gx = ex$ and, by the right cancellation rule, $g = e$.

An alternative proof involves multiplying both sides of the equation $gx = x$ on the right by the element x^{-1} .

- (b) We need to prove the following statement. Let G be a group with identity e and let x be an element of G . If g is an element of G such that $xg = x$, then $g = e$.

The proof is almost identical to that of part (a).

We are given that $xg = x$ and, by the identity axiom, we know that $xe = x$.

Hence $xg = xe$ and, by the left cancellation rule, $g = e$.

Solution to Exercise 1.4

We are given that $yx = e$ and, by the inverses axiom, we know that $x^{-1}x = e$. It follows that $yx = x^{-1}x (= e)$. Using the right cancellation rule, we have the required result that $y = x^{-1}$.

An alternative proof involves multiplying both sides of the equation $yx = e$ on the right by the element x^{-1} .

Solution to Exercise 1.5

- (a) Since composition of functions is applied from right to left, the functions compose as follows:

$$\begin{aligned} 1 &\mapsto 3 \mapsto 4 \\ 2 &\mapsto 5 \mapsto 2 \\ 3 &\mapsto 1 \mapsto 3 \\ 4 &\mapsto 2 \mapsto 5 \\ 5 &\mapsto 4 \mapsto 1. \end{aligned}$$

Thus

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 2 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 3 & 5 & 1 \end{pmatrix}.$$

- (b) We start by tracing the image of 1, the image of this image, and so on, until we come back to 1. Then we consider the first number not already used and repeat the process. This gives

$$\begin{aligned} 1 &\mapsto 3 \mapsto 4 \mapsto 1 \\ 2 &\mapsto 5 \mapsto 2. \end{aligned}$$

Hence the original permutation can be written in cycle form as $(1\,3\,4)(2\,5)$.

Since the cycles in cycle form are disjoint, the order of the cycles does not matter. So $(1\,3\,4)(2\,5)$ and $(2\,5)(1\,3\,4)$ are equivalent cycle forms for this permutation.

- (c) We start by tracing the image of 1, the image of the resulting number, and so on, until we come back to 1. Then we consider the first number not already used and repeat the process. As this is a product of cycles, we apply the cycles from right to left. We obtain the following.

$$\begin{array}{ccccccc} 1 & \xrightarrow{\quad} & 3 & \xrightarrow{\quad} & 3 & \xrightarrow{\quad} & 1 \\ & \underbrace{\hspace{1.5cm}} & & \underbrace{\hspace{1.5cm}} & & \underbrace{\hspace{1.5cm}} & \\ & (1\,3\,5\,6\,2) & & (2\,5\,4) & & (1\,6\,3) & \\ \\ 2 & \xrightarrow{\quad} & 1 & \xrightarrow{\quad} & 1 & \xrightarrow{\quad} & 6 \\ & \underbrace{\hspace{1.5cm}} & & \underbrace{\hspace{1.5cm}} & & \underbrace{\hspace{1.5cm}} & \\ & (1\,3\,5\,6\,2) & & (2\,5\,4) & & (1\,6\,3) & \\ \\ 6 & \xrightarrow{\quad} & 2 & \xrightarrow{\quad} & 5 & \xrightarrow{\quad} & 5 \\ & \underbrace{\hspace{1.5cm}} & & \underbrace{\hspace{1.5cm}} & & \underbrace{\hspace{1.5cm}} & \\ & (1\,3\,5\,6\,2) & & (2\,5\,4) & & (1\,6\,3) & \\ \\ 5 & \xrightarrow{\quad} & 6 & \xrightarrow{\quad} & 6 & \xrightarrow{\quad} & 3 \\ & \underbrace{\hspace{1.5cm}} & & \underbrace{\hspace{1.5cm}} & & \underbrace{\hspace{1.5cm}} & \\ & (1\,3\,5\,6\,2) & & (2\,5\,4) & & (1\,6\,3) & \\ \\ 3 & \xrightarrow{\quad} & 5 & \xrightarrow{\quad} & 4 & \xrightarrow{\quad} & 4 \\ & \underbrace{\hspace{1.5cm}} & & \underbrace{\hspace{1.5cm}} & & \underbrace{\hspace{1.5cm}} & \\ & (1\,3\,5\,6\,2) & & (2\,5\,4) & & (1\,6\,3) & \\ \\ 4 & \xrightarrow{\quad} & 4 & \xrightarrow{\quad} & 2 & \xrightarrow{\quad} & 2 \\ & \underbrace{\hspace{1.5cm}} & & \underbrace{\hspace{1.5cm}} & & \underbrace{\hspace{1.5cm}} & \\ & (1\,3\,5\,6\,2) & & (2\,5\,4) & & (1\,6\,3) & \end{array}$$

Hence the product $(1\,6\,3)(2\,5\,4)(1\,3\,5\,6\,2)$ can be written in cycle form as $(1)(2\,6\,5\,3\,4)$, or more simply as $(2\,6\,5\,3\,4)$, since the absence of a symbol implies that it is fixed.

Note that you do not need to show the details of the calculations in your answer. We have included them here to show what should be done in your head, but the answer can normally be written down directly.

Solution to Exercise 1.6

- (a) By the usual argument, corners must go to corners. Having moved one corner, there are only two places that an adjacent corner can be mapped to: the adjacent corners to the image corner. This gives a maximum of 12 symmetries.

There are six rotations about the centre O : through angles of 0 , $\frac{\pi}{3}$, $\frac{2\pi}{3}$, $\frac{3\pi}{3}$ ($= \pi$), $\frac{4\pi}{3}$ and $\frac{5\pi}{3}$ anticlockwise.

There are also six reflections: three in lines joining pairs of opposite corners, three in lines joining midpoints of opposite sides.

This shows that there are exactly 12 symmetries of a regular hexagon.

- (b) Since r is rotation through $\frac{\pi}{3}$, r^6 will be rotation through $\frac{6\pi}{3} = 2\pi$ and so correspond to the identity. Now $r^6 = e$ means that $r^{-1} = r^5$. The result $sr = r^5s$ now follows, since doing a rotation followed by a reflection is the equivalent of doing the reflection followed by the inverse of the rotation.

Solution to Exercise 1.7

Let G be a cyclic group generated by the element g . If x and y are any two elements of G , then for some integers m and n we have

$$x = g^m \quad \text{and} \quad y = g^n.$$

$$\begin{aligned} \text{Then } xy &= g^m g^n \\ &= g^{m+n} && \text{(by the rule of indices)} \\ &= g^{n+m} && \text{(since addition in } \mathbb{Z} \text{ is commutative)} \\ &= g^n g^m && \text{(by the rule of indices)} \\ &= yx. \end{aligned}$$

Hence G is abelian.

Solution to Exercise 1.8

We consider the multiples modulo 6 of each element.

- The multiples of 1 are 1, 2, 3, 4, 5 and 0, so 1 is a generator.
- The multiples of 2 are 2, 4 and 0, so 2 does not generate the group.
- The multiples of 3 are 3 and 0, so 3 does not generate the group.
- The multiples of 4 are 4, 2 and 0, so 4 does not generate the group.
- The multiples of 5 are 5, 4, 3, 2, 1 and 0, so 5 is a generator (for example, $5 + 5 + 5 = 15 \equiv 3 \pmod{6}$).

Solution to Exercise 1.9

From Example 1.9 we know that $4^2 \equiv 1 \pmod{5}$. Therefore the only powers of 4 modulo 5 are 4 and 1, and so 4 is not a generator.

Solution to Exercise 2.1

Recall that $S_3 = \{e, (12), (13), (23), (123), (132)\}$. We check that the conditions SG1, SG2 and SG3 hold for H .

The identity $e \in H$, so SG2 is satisfied.

As remarked, we need only check closure for pairs from $(123), (132)$. Since $(123)^2 = (132)$, $(132)^2 = (123)$, $(123)(132) = e$ and $(132)(123) = e$, condition SG1 is satisfied.

Finally, $(123)^{-1} = (132)$ and $(132)^{-1} = (123)$, so condition SG3 is satisfied.

Solution to Exercise 2.2

All subgroups must contain 0 (the identity), and any subgroup containing 1 or 5 is the whole group since both 1 and 5 are generators. The subgroups are as follows.

- The trivial subgroup $\{0\}$.
- The whole of $\mathbb{Z}_6$, that is, $\{0, 1, 2, 3, 4, 5\}$.
- $\{0, 2, 4\}$ – since 2 is in the group, $4 = 2 + 2 \pmod{6}$ must be as well. If we include either 3 or 5, we necessarily include 1 (since $3 + 4 = 5 + 2 \equiv 1 \pmod{6}$) and so we have the whole group.
- $\{0, 3\}$ – if we include either 2 or 4, we necessarily include 1 or 5 and so we have the whole group.

Solution to Exercise 2.3

We are given that H is a subgroup of the group G , so H satisfies the subgroup axioms. In particular, it is a subset of G .

Since it satisfies the identity axiom, H contains the identity element of G and so is non-empty. So H satisfies the first property.

Now suppose that x and y are any two elements of H . Since H satisfies the inverses axiom, and x is an element of H , we have that x^{-1} is an element of H . We now know that x^{-1} and y are elements of H . Being a subgroup, H satisfies the closure axiom, so the element $x^{-1}y$ is in H . So H satisfies the second property.

Solution to Exercise 2.4

For the ‘if’ part of the statement, we assume that H is a non-empty subset of G and that if x and y are in H then xy^{-1} is in H . We want to show that H is a subgroup of G , that is, that H satisfies the three subgroup axioms.

Identity By property (a), H is non-empty. Therefore there exists some element x in H . By property (b), if x and y are in H then xy^{-1} is in H . Taking $y = x$ shows that $xx^{-1} = e$ is in H .

Inverses If y is in H then, by the identity axiom (already verified), both e and y are in H . Property (b) then implies that $ey^{-1} = y^{-1}$ is in H .

Closure Let x and y be elements of H . By the inverses axiom (already verified), y^{-1} is an element of H . Therefore x and y^{-1} are both in H . So, by property (b), the product $x(y^{-1})^{-1} = xy$ is in H .

For the ‘only if’ part, we assume that H is a subgroup of the group G , so it satisfies the subgroup axioms. In particular, H is a subset of G .

Since it satisfies the identity axiom, H contains the identity element of G and so is non-empty. So H satisfies property (a).

Now suppose that x and y are any two elements of H . Since H satisfies the inverses axiom, and y is an element of H , so is the element y^{-1} . We now know that x and y^{-1} are elements of H . Since H is a subgroup, it satisfies the closure axiom, so the element xy^{-1} is in H . So H satisfies property (b).

Solution to Exercise 2.5

- (a) From the definition of a subgroup, the underlying set of K is a subset of the underlying set of H and hence of the underlying set of G . Furthermore K forms a group under the same group operation as H and hence, since H is a subgroup of G , under that of G . Thus K is a subgroup of G .
- (b) This follows immediately from the definition since H and K both form groups under the same operation as G .

Solution to Exercise 2.6

We saw in Exercise 2.2 that the group $\mathbb{Z}_6$ under addition modulo 6 has subgroups $\{0, 3\}$ and $\{0, 2, 4\}$, and the union of these is $\{0, 2, 3, 4\}$.

This set is not a subgroup since it is not closed under addition modulo 6. For example, $2 + 3 \equiv 5 \pmod{6}$ is not in the set.

An alternative reason why the set is not a subgroup is provided by a theorem due to Joseph-Louis Lagrange (1736–1813), which you will meet in Subsection 2.2, since the subset has four elements and 4 does not divide 6.

Solution to Exercise 2.7

Using additive notation, if H is a subgroup of the abelian group G then

$$x + y = y + x$$

for all $x, y \in G$ and, as H is a subset of G , certainly

$$x + y = y + x$$

for all $x, y \in H$.

Solution to Exercise 2.8

Recall that $S_3 = \{e, (12), (13), (23), (123), (132)\}$. Then the cosets of $\{e, (12)\}$ are as follows.

- $e\{e, (12)\} = \{e, (12)\}$
- $(12)\{e, (12)\} = \{(12), (12)(12)\} = \{(12), e\}$
- $(13)\{e, (12)\} = \{(13), (13)(12)\} = \{(13), (123)\}$
- $(23)\{e, (12)\} = \{(23), (23)(12)\} = \{(23), (132)\}$
- $(123)\{e, (12)\} = \{(123), (123)(12)\} = \{(123), (13)\}$
- $(132)\{e, (12)\} = \{(132), (132)(12)\} = \{(132), (23)\}$

Thus there are just three distinct left cosets, namely

$$\{e, (12)\}, \quad \{(13), (123)\} \quad \text{and} \quad \{(23), (132)\}.$$

Solution to Exercise 2.9

We are given that $aH = bH$ and we must show that $a^{-1}b \in H$.

Since $b = be$, the element b is in the coset bH . But $aH = bH$, so $b \in aH$. Therefore there exists some $h \in H$ such that $b = ah$.

So $a^{-1}b = a^{-1}ah = h$, and therefore $a^{-1}b$ is in H .

Solution to Exercise 2.10

- (a) To show that f is one-one, suppose that $f(x) = f(y)$. Then by the definition of f we have that

$$ax = ay.$$

Then $x = y$ by left cancellation. Hence f is one-one.

To show that f is onto, let z be any element in the codomain aH , so that $z = ah$ for some $h \in H$. Then by the definition of f we have $z = f(h)$. Hence f is onto.

- (b) By part (a), the left cosets aH and bH each have the same number of elements as the subgroup H .

Solution to Exercise 2.11

Since $|S_3| = 6$, by Lagrange's Theorem we know that the possible sizes of subgroups of S_3 are 1, 2, 3 and 6. Here is a complete list:

- $\{e\}$, the trivial subgroup
- S_3 , the whole group
- $\{e, (1\ 2)\}$, a subgroup of order 2
- $\{e, (1\ 3)\}$, a subgroup of order 2
- $\{e, (2\ 3)\}$, a subgroup of order 2
- $\{e, (1\ 2\ 3), (1\ 3\ 2)\}$, a subgroup of order 3.

Solution to Exercise 2.12

By Proposition 2.6, $H \cap K$ is a subgroup of both H and K . By Lagrange's Theorem, the order of $H \cap K$ must divide both $|H|$ and $|K|$. But $|H|$ and $|K|$ are coprime, that is, their highest common factor is 1. This implies that $|H \cap K| = 1$ and so $H \cap K = \{e\}$.

Solution to Exercise 3.1

Since $\phi(aH)$ is defined in terms of a particular element a of the coset aH , and not in terms of aH itself, to show that ϕ is well defined we must show that if $aH = bH$ then $\phi(aH) = \phi(bH)$, that is, $Ha^{-1} = Hb^{-1}$.

Suppose that $aH = bH$. By Proposition 3.1, we have

$$Ha^{-1} = Hb^{-1} \quad \text{if, and only if,} \quad a^{-1}(b^{-1})^{-1} \in H.$$

But $a^{-1}(b^{-1})^{-1} = a^{-1}b$, and we know that $a^{-1}b \in H$ by our assumption that $aH = bH$ and Proposition 2.11. Therefore $Ha^{-1} = Hb^{-1}$, and so ϕ is well defined.

To show that ϕ is one-one, suppose that $\phi(aH) = \phi(bH)$, that is, $Ha^{-1} = Hb^{-1}$. From Proposition 3.1, we have that

$$a^{-1}(b^{-1})^{-1} = a^{-1}b \in H.$$

Therefore $aH = bH$ by Proposition 2.11, and so ϕ is one-one.

Finally, suppose that Hx is any right coset of H in G . Then $x^{-1} \in G$ and

$$\phi(x^{-1}H) = H(x^{-1})^{-1} = Hx.$$

This shows that ϕ is onto.

Solution to Exercise 3.2

- (a) We already know by Proposition 2.3 that both $\{e\}$ and G are subgroups of G .

If a is any element of G , then

$$a\{e\} = \{e\}a = \{a\}.$$

Hence $\{e\}$ is a normal subgroup of G .

To show that G is a normal subgroup of G , we show that if a is any element of G , then aG and Ga are both equal to G .

Since $a \in G$, Proposition 2.10 gives $aG = G$. By the corresponding result for right cosets, $Ga = G$. So for all $a \in G$, we have $aG = Ga = G$, and hence G is a normal subgroup of G .

- (b) Suppose that H is a subgroup of the abelian group G and that $a \in G$.

The normality condition in additive notation is $a + H = H + a$ for all $a \in H$.

Any element of $a + H$ can be written as $a + h$ for some $h \in H$. Since G is abelian, $a + h = h + a$. This tells us that every element of $a + H$ is an element of $H + a$. Therefore

$$a + H \subseteq H + a.$$

Similarly,

$$H + a \subseteq a + H,$$

and equality follows. Hence H is a normal subgroup of G .

Solution to Exercise 3.3

- (a) By Exercise 2.1, we know that H is a subgroup of G . By Exercise 2.10, H has two left cosets, namely H and $(1\ 2)H = \{(1\ 2), (1\ 3), (2\ 3)\}$. Similarly, H has two right cosets, namely H and $H(1\ 2) = \{(1\ 2), (1\ 3), (2\ 3)\}$. Since the left cosets of H are the same as the right cosets, H is a normal subgroup of G by Proposition 3.7(b).

- (b) By the definition of index, H has exactly two left cosets and exactly two right cosets in G . One left (respectively right) coset of H is H itself.

From the proof of Lagrange's Theorem, we know that the left (respectively right) cosets of H in G form a partition of G . Therefore the other left (respectively right) coset is the difference $G \setminus H$. So the set of left cosets of H is the same as the set of right cosets, and the result follows by Proposition 3.7(b).

- (c) Let N be the intersection of the given collection of normal subgroups of G . By Proposition 2.7, N is a subgroup of G .

Now suppose that H is any normal subgroup in the collection. Since $N \subseteq H$, by Proposition 3.7(a)

$$\begin{aligned} aNa^{-1} &\subseteq aHa^{-1} \\ &\subseteq H. \end{aligned}$$

This argument shows that aNa^{-1} is contained in *every* subgroup of the collection, and hence is contained in the intersection of the collection. That is,

$$aNa^{-1} \subseteq N,$$

and so N is a normal subgroup of G by Proposition 3.7(a).

Solution to Exercise 3.4

We use the subgroup criterion (Proposition 2.4).

To see that gHg^{-1} is not empty, note that $e \in H$ and so $geg^{-1} \in gHg^{-1}$.

Now let $x, y \in gHg^{-1}$. Then $x = gh_1g^{-1}$ and $y = gh_2g^{-1}$ for some $h_1, h_2 \in H$. Thus

$$x^{-1}y = (gh_1g^{-1})^{-1}gh_2g^{-1} = gh_1^{-1}g^{-1}gh_2g^{-1} = g(h_1^{-1}h_2)g^{-1} \in gHg^{-1}.$$

Therefore gHg^{-1} is a subgroup of G .

Solution to Exercise 3.5

To show that $\sim$ is an equivalence relation, we need to show that it is reflexive, symmetric and transitive.

Since $a = eae^{-1}$ for all $a \in G$, any element a is conjugate to itself. This shows that $\sim$ is reflexive.

To see that $\sim$ is symmetric, suppose that $a \sim b$, so that $b = gag^{-1}$ for some $g \in G$. Then

$$g^{-1}bg = g^{-1}gag^{-1}g = eae = a,$$

hence $g^{-1}b(g^{-1})^{-1} = a$. Thus $b \sim a$.

For transitivity, suppose that $a \sim b$ and $b \sim c$. Then $b = gag^{-1}$ and $c = hbg^{-1}$ for some $g, h \in G$. Thus $c = hgag^{-1}h^{-1} = (hg)a(hg)^{-1}$, and so $a \sim c$.

Solution to Exercise 3.6

There are three conjugacy classes in S_3 , namely

$$\{e\}; \{(12), (13), (23)\}; \{(123), (132)\}.$$

Solution to Exercise 3.7

- (a) Using the definition of the product of two cosets, and the associativity axiom for the group G , we have

$$\begin{aligned}
 aN(bNcN) &= aN(bcN) \\
 &= a(bc)N \\
 &= (ab)cN \\
 &= (ab)NcN \\
 &= (aNbN)cN.
 \end{aligned}$$

- (b) As remarked, $N = eN$. So, for any element $aN \in G/N$, we have

$$NaN = eNaN = (ea)N = aN.$$

Similarly, $aNN = aN$. Hence N is the identity element of G/N .

- (c) By the definition of the product in G/N ,

$$a^{-1}NaN = (a^{-1}a)N = eN = N.$$

Similarly,

$$aNaa^{-1}N = (aa^{-1})N = eN = N.$$

Hence $a^{-1}N$ is the inverse of aN .

Solution to Exercise 3.8

As usual, we need to prove two set inclusions. For convenience, let

$$P = \{xy : x \in aN, y \in bN\} \quad \text{and} \quad Q = \{(ab)n : n \in N\}.$$

Firstly we show that $P \subseteq Q$. Let z be an element of P . Then $z = an_1bn_2$ for some n_1 and n_2 in N . Now n_1b is an element of Nb . Since N is a normal subgroup, we know that $Nb = bN$, so $n_1b = bn_3$ for some n_3 in N . Therefore $z = an_1bn_2 = abn_3n_2$, which is an element of Q . This shows that $P \subseteq Q$.

To show that $Q \subseteq P$, let z be an element of Q , so $z = abn$ for some n in N . But a is in aN and bn is in bN . Therefore $z = (a)(bn)$ is in P . This shows that $Q \subseteq P$.

Hence $P = Q$.

Solution to Exercise 3.9

(a) There are three cosets of H in S_3 :

$$A = \{e, (12)\}, B = \{(123), (13)\} \text{ and } C = \{(132), (23)\}.$$

(b) Consider the elements of B and C . We have

$$\underbrace{(123)}_{\in B} \underbrace{(132)}_{\in C} = e \in A, \text{ and}$$

$$\underbrace{(13)}_{\in B} \underbrace{(23)}_{\in C} = (132) \in C.$$

So the products of an element from B and an element from C are not necessarily in the same coset. This means that the product BC is not well defined.

Solution to Exercise 3.10

(a) $N = \{e, (123), (132)\}$

(b) The elements of G/N are $eN = N$ and $(12)N = \{(12), (13), (23)\}$.

The Cayley table is below.

$\circ$	N	$(12)N$
N	N	$(12)N$
$(12)N$	$(12)N$	N

You may have used different notation for the second coset. This is fine.

Notice that another way of writing the Cayley table is

$\circ$	even	odd
even	even	odd
odd	odd	even

where ‘even’ stands for the coset containing the even permutations and ‘odd’ stands for the coset containing the odd permutations.

Solution to Exercise 4.1

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Solution to Exercise 4.2

Since $r^4 = e$, we have $R = \langle r \rangle = \{e, r, r^2, r^3\}$. The Cayley table of R is as follows.

$\circ$	e	r	r^2	r^3
e	e	r	r^2	r^3
r	r	r^2	r^3	e
r^2	r^2	r^3	e	r
r^3	r^3	e	r	r^2

Remember that a subgroup of index 2 is always normal – see Exercise 3.3.

Solution to Exercise 4.3

It is clear that ϕ is a function from $\mathbb{Z}$ to $2\mathbb{Z}$. We need to check that ϕ is a bijection and that it preserves the binary operation.

To check that ϕ is one-one, let $\phi(a) = \phi(b)$ for $a, b \in \mathbb{Z}$. Then $2a = 2b$, which implies that $a = b$. Therefore ϕ is one-one.

To show that ϕ is onto, let a be any element of $2\mathbb{Z}$. Then $a = 2m$ for some $m \in \mathbb{Z}$. Hence $a = \phi(m)$, proving that ϕ is onto.

Finally, we check that ϕ preserves the binary operation:

$$\begin{aligned}\phi(a + b) &= 2(a + b) \\ &= 2a + 2b \\ &= \phi(a) + \phi(b).\end{aligned}$$

Solution to Exercise 4.4

Since $aa^{-1} = e$ and ϕ is an isomorphism, we have that $\phi(a)\phi(a^{-1}) = \phi(e)$.

But $\phi(e)$ is the identity of H (by Theorem 4.3), so $\phi(a^{-1})$ behaves like the right inverse of $\phi(a)$ in H .

Now Proposition 1.6 gives that $\phi(a^{-1})$ is the inverse of $\phi(a)$ in H , that is,

$$(\phi(a))^{-1} = \phi(a^{-1}).$$

Solution to Exercise 4.5

In $\mathbb{Z}_5^*$ we have that $3^2 \equiv 4$, $3^3 \equiv 2$ and $3^4 \equiv 1$. Hence the element 3 is a generator of the group.

Since 1 is a generator of $\mathbb{Z}_4$, we might look for an isomorphism ϕ from $\mathbb{Z}_4$ to $\mathbb{Z}_5^*$ for which $\phi(1) = 3$.

The inverse of 1 in $\mathbb{Z}_4$ is 3 and the inverse of 3 in $\mathbb{Z}_5^*$ is 2, so we also need $\phi(3) = 2$. Since we know that we must have $\phi(0) = 1$, this leaves $\phi(2) = 4$.

Rewriting the Cayley table as

$\times_5$	1	3	4	2
1	1	3	4	2
3	3	4	2	1
4	4	2	1	3
2	2	1	3	4

we find that it does have the same pattern as the Cayley table for $(\mathbb{Z}_4, +_4)$, and so the function ϕ defined by

$$\phi(0) = 1, \phi(1) = 3, \phi(2) = 4, \phi(3) = 2$$

is an isomorphism from $\mathbb{Z}_4$ to $\mathbb{Z}_5^*$.

Solution to Exercise 4.6

- (a) To show that the group H is abelian we must show that $xy = yx$ for any x and y in H .

Since ϕ is onto, for x and y in H there are elements a and b in G such that $\phi(a) = x$ and $\phi(b) = y$.

Now G is an abelian group, so $ab = ba$. Therefore, since ϕ is an isomorphism, we have

$$\begin{aligned} xy &= \phi(a)\phi(b) \\ &= \phi(ab) \\ &= \phi(ba) \\ &= \phi(b)\phi(a) \\ &= yx. \end{aligned}$$

Hence H is abelian.

- (b) Since $\mathbb{Z}_6$ is an abelian group and S_3 is not, these groups cannot be isomorphic.

Solution to Exercise 4.7

Since $g^n = e$, the order of g must be finite by Definition 4.4. Suppose that the order of g is m . Then $m \leq n$, so by the Division Algorithm (Book A, Chapter 1, Theorem 4.1) there are $q, r \in \mathbb{N}$ with $n = qm + r$ and $0 \leq r < m$. Then, since $g^m = e$, we have $g^{qm} = e$, so that $e = g^n = g^{qm}g^r$ gives $g^r = e$. Since $r < m$, by definition of order we get $r = 0$. But then $n = qm$; that is, the order of g divides n , as required.

Solution to Exercise 4.8

Let $g \in G$, where $g \neq e$. Then by Proposition 4.5 the order of g must divide p . Since p is prime and we have assumed $g \neq e$, the order of g must be p . Hence G is cyclic and generated by g .

Solution to Exercise 4.9

Suppose that $\phi(a)$ has finite order n . By Proposition 4.2 the inverse ϕ^{-1} is an isomorphism, so by Theorem 4.6 $\phi^{-1}(\phi(a)) = a$ also has finite order n .

We have shown that if $\phi(a)$ has finite order, so does a . This is equivalent to showing that if a has infinite order, so does $\phi(a)$.

Solution to Exercise 4.10

- (a) We know from the definition that ϕ is a function from $\mathbb{Z}$ to $\mathbb{Z}$. Furthermore, for all m and n in the domain $\mathbb{Z}$,

$$\phi(m+n) = 3(m+n) = 3m+3n = \phi(m) + \phi(n).$$

Hence ϕ has the morphism property and so it is a homomorphism from $(\mathbb{Z}, +)$ to itself.

However, ϕ is not an isomorphism, since it is not onto. For example, the element 1 of the codomain is not in the image set of ϕ .

- (b) The kernel consists of all elements that map to the identity of the codomain, which is 0. Thus it consists of all $n \in \mathbb{Z}$ such that

$$\phi(n) = 3n = 0.$$

The only possibility is $n = 0$. Thus

$$\text{Ker}(\phi) = \{0\},$$

which is, trivially, a subgroup of the domain.

- (c) The elements of the image are those integers of the form $\phi(n) = 3n$ for some $n \in \mathbb{Z}$. Hence

$$\text{Im}(\phi) = \{3n : n \in \mathbb{Z}\} = 3\mathbb{Z}.$$

Now $3\mathbb{Z}$ is a non-empty set, since $0 \in 3\mathbb{Z}$. Also, if $3m$ and $3n$ are any two elements of $3\mathbb{Z}$, then

$$3m - 3n = 3(m - n) \in 3\mathbb{Z}.$$

Thus $3\mathbb{Z}$ is a subgroup of the codomain $\mathbb{Z}$, by Proposition 2.5.

Solution to Exercise 4.11

- (a) Let $a, b \in \phi(G)$. Then $a = \phi(g)$ and $b = \phi(k)$ for some $g, k \in G$. Thus

$$ab = \phi(g)\phi(k) = \phi(gk) = \phi(kg) = \phi(k)\phi(g) = ba.$$

Hence $\phi(G)$ is abelian.

- (b) Since g has order n , we know that $g^n = e_G$ and hence

$$(\phi(g))^n = \phi(g^n) = \phi(e_G) = e_H,$$

where e_G is the identity in G and e_H is the identity in H . The required result follows by Exercise 4.7.

Solution to Exercise 4.12

Let G be an abelian group. Then a quotient of G has the form G/N for some subgroup N of G (we know that since G is abelian, all its subgroups are normal).

By Theorem 4.15, there is a homomorphism ϕ from G onto the quotient group G/N . Since G is abelian, so is $\phi(G)$ by Exercise 4.11. But $\phi(G) \cong G/N$, which gives the required result.

Solution to Exercise 4.13

Firstly, we show that H contains N (and is thus non-empty). The coset $eN = N$ is the identity of the quotient group G/N and so is an element of the subgroup $\overline{H}$. Therefore, by the definition of H , we have $e \in H$ and so H is non-empty.

Furthermore, $nN = N$ for every $n \in N$. So, by the definition of H , we have $n \in H$ for every $n \in N$. Hence

$$N \subseteq H.$$

Now let a and b be elements of H . We will show that $a^{-1}b$ is in H . By the definition of H , the cosets aN and bN are elements of $\overline{H}$, which is a subgroup of G/N . It follows that $\overline{H}$ also contains

$$\begin{aligned}(aN)^{-1}(bN) &= (a^{-1}N)(bN) \\ &= (a^{-1}b)N.\end{aligned}$$

From the definition of H , this means that $a^{-1}b \in H$. Therefore $H \leq G$ by Proposition 2.4.

Solution to Exercise 5.1

- (a) (i) $(1\ 3)$; (ii) $(1\ 4)(2\ 3)$; (iii) $(1\ 2)(3\ 4)$; (iv) $(1\ 2\ 3\ 4)$; (v) e .
 (b) (i) $(1\ 3)$; (ii) $(1\ 4)(2\ 3)$; (iii) $(1\ 2)(3\ 4)$; (iv) $(1\ 4\ 3\ 2)$; (v) e .

Solution to Exercise 5.2

- (i) By inspection we see that H_1 contains all the symmetries of Figure 5.2(c), hence it is a group under composition of permutations. Similarly:
 (ii) H_2 is the symmetry group for Figure 5.2(a), and the group of direct symmetries of Figure 5.2(e).
 (iii) H_3 is the symmetry group for Figure 5.2(e).
 (iv) H_4 is the symmetry group for Figure 5.2(b).
 (v) H_5 is the symmetry group for Figure 5.2(d).

Solution to Exercise 5.3

We know from Example 5.1 that each left coset of H_3 in S_4 contains elements that are determined by where 2 maps *to*. Similarly, the elements of a given right coset of H_3 will be determined by the element that 2 maps *from*. More specifically:

- every element of $H_3(1\ 2)$ sends 1 to 2
- every element of $H_3(2\ 3)$ sends 3 to 2
- every element of $H_3(2\ 4)$ sends 4 to 2.

Solution to Exercise 5.4

- (a) The positive divisors of 24 are 1, 2, 3, 4, 6, 8, 12 and 24, so by Lagrange's Theorem these are the possible orders of the subgroups of S_4 .
- (b) One cycle structure is that of the identity. Only e has this cycle structure, and it has order 1. A complete answer is given in the table below.

Representative of cycle structure	Number of elements	Order
e	1 element	1
$(1\ 2)$	6 elements	2
$(1\ 2\ 3)$	8 elements	3
$(1\ 2\ 3\ 4)$	6 elements	4
$(1\ 2)(3\ 4)$	3 elements	2

- (c) From part (b), we know that S_4 has

- one element of order 1
- nine elements of order 2
- eight elements of order 3
- six elements of order 4.

Solution to Exercise 5.5

- (a) (i) $(2\ 4)$ (ii) $(1\ 3\ 2\ 4)$
- (b) $g_1 = (1\ 2\ 4)$ or $(1\ 2\ 4\ 3)$ or $(1\ 4)$ or $(1\ 4\ 3)$;
 $g_2 = (2\ 3\ 4)$ or $(1\ 3\ 2\ 4)$ or $(1\ 4\ 3)$ or $(1\ 2)$.
- (c) There are five conjugacy classes, whose elements are described in the table in the solution to Exercise 5.4(b).

Solution to Exercise 5.6

- (a) There are nine subgroups of order 2, each of them generated by a different element of order 2. On the other hand, each subgroup of order 3 contains two elements of order 3, so there are four such subgroups, each consisting of the identity and two elements of order 3:

$$\begin{aligned} &\{e, (1\ 2\ 3), (1\ 3\ 2)\}, \\ &\{e, (1\ 2\ 4), (1\ 4\ 2)\}, \\ &\{e, (1\ 3\ 4), (1\ 4\ 3)\}, \\ &\{e, (2\ 3\ 4), (2\ 4\ 3)\}. \end{aligned}$$

- (b) The cyclic subgroups of order 4 are those generated by an element of order 4, that is,

$$\begin{aligned} &\{e, (1\ 2\ 3\ 4), (1\ 3)(2\ 4), (1\ 4\ 3\ 2)\}, \\ &\{e, (1\ 3\ 2\ 4), (1\ 2)(3\ 4), (1\ 4\ 2\ 3)\}, \\ &\{e, (1\ 2\ 4\ 3), (1\ 4)(2\ 3), (1\ 3\ 4\ 2)\}. \end{aligned}$$

- (c) Since all the non-identity elements of V have order 2, V is not cyclic (no element can be a generator). Observe that $V = H_5$ in Exercise 5.2.

The subgroup V is isomorphic to all non-cyclic subgroups of order 4 in S_4 , namely to $\{e, (12), (34), (12)(34)\}$ (note that this is H_4 in Exercise 5.2), $\{e, (13), (24), (13)(24)\}$, $\{e, (14), (23), (14)(23)\}$ and V itself.

Since any group of order 4 is either cyclic or isomorphic to V , these subgroups and the ones in part (b) are in fact all the subgroups of order 4.

- (d) In Exercise 5.4 we saw that S_4 does not contain any elements of order 6, so S_4 does not contain a cyclic subgroup of order 6.
- (e) The subgroup H_3 consists of those permutations in S_4 that fix the symbol 2 – that is, they map 2 to 2. We obtain isomorphic groups by considering the three sets that consist of those permutations that fix the symbols 1, 3 and 4 respectively:

$$\{e, (23), (24), (34), (234), (243)\},$$

$$\{e, (12), (14), (24), (124), (142)\},$$

$$\{e, (12), (13), (23), (123), (132)\}.$$

- (f) There are no cyclic subgroups of S_4 of order 8 because S_4 has no elements of order 8.

If we represent the symmetries of a square as a group of permutations of the vertices of the square, we obtain a subgroup of S_4 with order 8, namely

$$D_4 = \{e, (13), (24), (13)(24), (12)(34), (14)(23), (1234), (1432)\}.$$

If we interchange the symbols 2 and 3 in each permutation in D_4 (this corresponds to ordering the vertices of the square in a slightly unnatural way!), we obtain another subgroup of order 8:

$$\{e, (12), (34), (12)(34), (13)(24), (14)(23), (1324), (1423)\}.$$

Similarly, interchanging 3 and 4 in D_4 gives

$$\{e, (14), (23), (14)(23), (12)(34), (13)(24), (1243), (1342)\}.$$

- (g) The subgroup A_4 of even permutations of S_4 has order 12.

Solution to Exercise 5.7

H_2 is the group of direct symmetries of the tetrahedron that fix vertex 2.

H_3 is the subgroup of $\Gamma(\text{TET})$ fixing vertex 2.

A_4 is the subgroup of direct symmetries of $\Gamma(\text{TET})$.

Solution to Exercise 5.8

- (a) $(1\ 2)H_3(1\ 2)^{-1} = (1\ 2)H_3(1\ 2) = \{e, (2\ 3), (2\ 4), (3\ 4), (2\ 3\ 4), (2\ 4\ 3)\}.$
 $(1\ 3\ 2\ 4)H_4(1\ 3\ 2\ 4)^{-1} = (1\ 3\ 2\ 4)H_4(1\ 4\ 2\ 3) = H_4.$
- (b) The subgroups H_4 and H_5 are not conjugate because $(1\ 2) \in H_4$ is not conjugate to any element in H_5 .
- (c) No: for example, the subgroup $\{e, (1\ 2)\}$ is not conjugate to $\{e, (1\ 2)(3\ 4)\}.$
- (d) Yes. We have

$$\begin{aligned} (1\ 2)\{e, (1\ 3\ 4), (1\ 4\ 3)\}(1\ 2)^{-1} &= \{e, (2\ 3\ 4), (2\ 4\ 3)\}, \\ (1\ 4)\{e, (2\ 3\ 4), (2\ 4\ 3)\}(1\ 4)^{-1} &= \{e, (1\ 2\ 3), (1\ 3\ 2)\}, \\ (3\ 4)\{e, (1\ 2\ 3), (1\ 3\ 2)\}(3\ 4)^{-1} &= \{e, (1\ 2\ 4), (1\ 4\ 2)\}, \\ (2\ 3)\{e, (1\ 2\ 4), (1\ 4\ 2)\}(2\ 3)^{-1} &= \{e, (1\ 3\ 4), (1\ 4\ 3)\}. \end{aligned}$$

These conjugacy relations suffice to establish that all four subgroups of S_4 of order 3 are conjugate to one another.

Solution to Exercise 5.9

From Proposition 3.12, we know that a normal subgroup N of S_4 must be a union of conjugacy classes, which must include the class $\{e\}$. Therefore $|N|$ will be the sum of the sizes of these conjugacy classes. Moreover, by Lagrange's Theorem, this sum must divide 24.

We know from Exercise 5.4 that the conjugacy classes of S_4 have sizes 1, 3, 6 and 8. The only ways to add any of these numbers in such a way that one of the summands is 1 and the sum is a proper divisor of 24 are $1 + 3 = 4$ and $1 + 3 + 8 = 12$. Therefore a non-trivial normal subgroup of S_4 can only have size 4 or 12.

A normal subgroup of size 4 is the Klein subgroup $V = \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$. A normal subgroup of size 12 is the alternating group A_4 .

Solution to Exercise 5.10

- (a) Suppose that ϕ is a group homomorphism with domain S_4 and such that $\text{Ker}(\phi) = A_4$. Then $S_4/A_4 \cong \text{Im}(\phi)$ by the First Isomorphism Theorem.

Since $|A_4| = 12$, the index of A_4 in S_4 is 2; that is, $|S_4/A_4| = 2$. So $\text{Im}(\phi)$ contains exactly two elements.

- (b) The mapping $\phi : S_4 \rightarrow \mathbb{Z}_2$ defined by

$$\phi(\sigma) = \begin{cases} 0, & \text{if } \sigma \text{ is an even permutation,} \\ 1, & \text{otherwise} \end{cases}$$

is a homomorphism whose kernel is A_4 .

Solution to Exercise 5.11

- (a) Lagrange's Theorem gives 1, 2, 3, 4, 6 and 12 as possible orders of subgroups of A_4 .
- (b) A subgroup of A_4 is automatically a subgroup of S_4 , so we seek those subgroups of S_4 that contain only even permutations. The trivial subgroup $\{e\}$ is one such subgroup, and it has order 1. Moreover, using the results in Exercise 5.6 we find
- three subgroups of order 2, such as $\{e, (12)(34)\}$
 - four subgroups of order 3, such as $\{e, (123), (132)\}$
 - the Klein subgroup V , of order 4
 - the group A_4 itself, of order 12.

There is no subgroup of order 6, which shows that the converse of Lagrange's Theorem is false.

- (c) We see by inspection that there is no element $g \in A_4$ such that $g(123)g^{-1} = (234)$. Therefore the permutations (123) and (234) are *not* conjugate in A_4 .

Note that in S_4 there are three such g , namely (1234) , (1324) and (14) , but these are odd permutations and hence not in A_4 .

- (d) There are four conjugacy classes in A_4 , namely

$$\begin{aligned} &\{e\}, \\ &\{(123), (142), (134), (243)\}, \\ &\{(132), (124), (143), (234)\}, \\ &\{(12)(34), (13)(24), (14)(23)\}. \end{aligned}$$

- (e) The only non-trivial, proper normal subgroup of A_4 is the Klein subgroup V . Note that any subgroup of A_4 that is normal in S_4 will necessarily be normal in A_4 .

Solution to Exercise 5.12

	S_4	A_4
(a) order of group	24	12
(b) number of subgroups of order 2	9	3
(c) number of subgroups of order 3	4	4
(d) number of cyclic subgroups of order 4	3	0
(e) number of non-cyclic subgroups of order 4	4	1
(f) number of cyclic subgroups of order 6	0	0
(g) number of non-cyclic subgroups of order 6	4	0
(h) number of subgroups of order 8	3	0
(i) number of subgroups of order 12	1	1
(j) total number of subgroups	30	10
(k) total number of normal subgroups	4	3

Note that the trivial subgroup $\{e\}$ and the whole group are counted in parts (j) and (k).

Solution to Exercise 5.13

